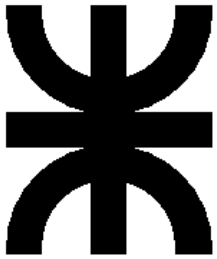

UNIVERSIDAD TECNOLOGICA NACIONAL

FACULTAD REGIONAL SAN NICOLAS

INGENIERIA EN ELECTRONICA

PROBLEMA DE INGENIERÍA

TECNICAS DIGITALES III

CONFIGURACIÓN AVANZADA DE REDES LAN

Integrantes:

- Bertero Gabriel
- Valentini Jorge

Docentes:

- Profesor: Poblete Felipe
- Auxiliar: González Mariano

AÑO 2011

Problema de Ingeniería - Técnicas Digitales III

18 DE DICIEMBRE DE 2011

Configuración Avanzada de Redes LAN

Gabriel BERTERO

Jorge VALENTINI

Universidad Tecnológica Nacional - Facultad Regional San Nicolás

Este documento está preparado para su impresión a doble cara. Seamos responsables en el uso de los recursos naturales

Configuración Avanzada de Redes LAN

Problema de Ingeniería

Gabriel BERTERO y Jorge VALENTINI

Técnicas Digitales III
Universidad Tecnológica Nacional
Facultad Regional San Nicolás

18 de Diciembre de 2011

Índice

Parte I

Introducción y Conceptos Previos

En esta parte del documento se presenta el anteproyecto, se explica el por qué de la elección, y se muestra un bosquejo del diseño del trabajo final. Además se introduce al lector en los conceptos mínimos que requerirá para poder seguir el trabajo

Capítulo 1

Propuesta

Orientamos nuestro problema al diseño de redes y seguridad informática, creemos que hoy en día todo servicio que pueda brindar un área de electrónica, llegará tarde o temprano a requerir el uso de una red de datos. Si bien muchos electrónicos solicitarán ayuda al personal con experiencia en el tema, pretendemos que este proyecto sirva como un material de consulta para aquellos que deban incluir redes de datos en su trabajo y deseen diseñarlas y ponerlas en marcha, o bien quieran hacer una depuración ante fallas de un sistema. Si bien en la carrera se "tocan" cuestiones teóricas sobre redes de datos, nunca se muestra el paso a paso del diseño y configuración de una red "desde cero".

Nos enfocamos en una infraestructura de red compleja con el objeto de abarcar la mayor cantidad de conceptos posibles a fin de que sirva como guía en una gran variedad de escenarios simples y algunos escenarios complejos.

Para mostrar un diagrama (solo funcional, mas adelante se mostrará un diagrama formal: Figura 7.1, página 70) y dar forma a la red consideremos el siguiente bosquejo:

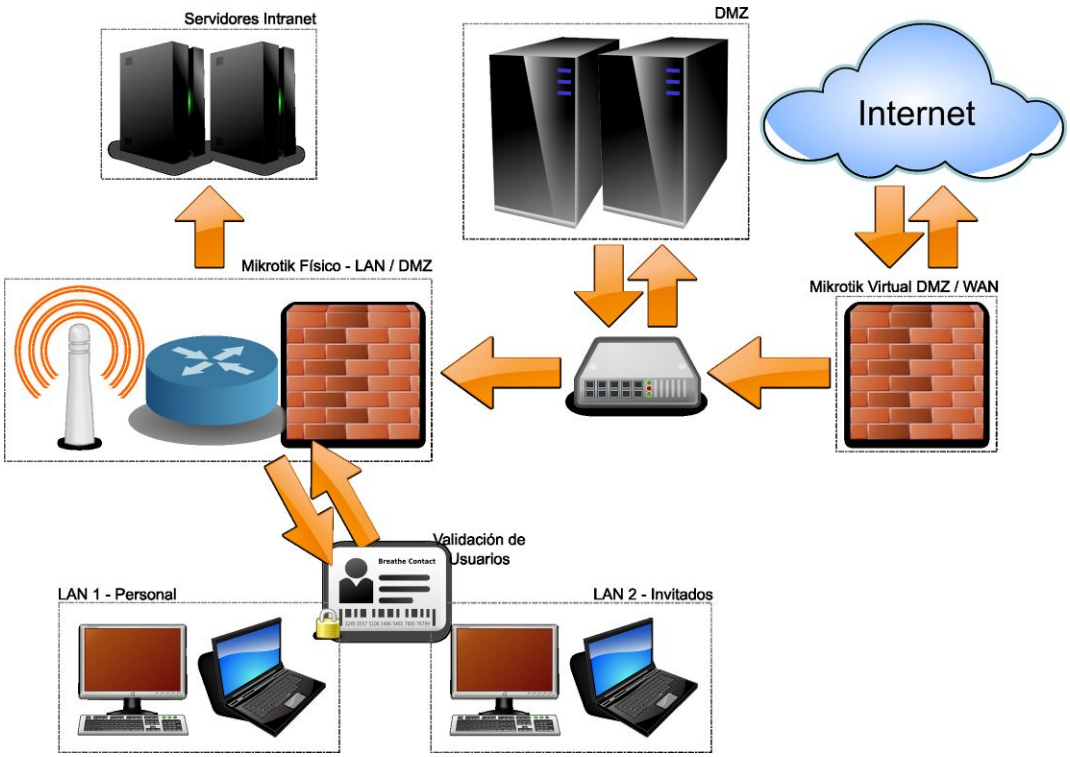

Figura 1.1: Diagrama funcional de la red

Se generará un modelo real de la red propuesta para poder probar la seguridad, y se generará un informe teórico de todos los conceptos abarcados en el proyecto: DMZ, LAN, WAN, VPN, Firewall, etc. El modelo real utilizará en mayor medida equipos virtuales, esto tiene la intención de dejar en evidencia la potencia de trabajar en un ambiente virtualizado, tanto para laboratorios como para ambientes productivos.

1.1. Incumbencias de Técnicas Digitales III

El proyecto abarca los siguientes temas de Técnicas Digitales 3:

- Virtualización
- Infraestructura de redes
- Seguridad Informática

1.2. Materias Abarcadas

En este problema, incluimos además conocimientos que incumben a otras materias de la curricula de Ingeniería Electrónica:

Medios De Enlace Enlaces inalámbricos, modelo OSI, redes Canopy

Sistemas de Comunicaciones II Ethernet, IP, Redes industriales,

1.3. Entrevista a un Profesor

El ingeniero Sebastián Schaller, profesor de Electrónica Aplicada III y Sistemas de Comunicaciones II, nos enseña a los estudiantes de electrónica las nociones sobre redes de datos, redes industriales (Profibus, Profinet, etc.), entre otras tecnologías como SDH, ATM, etc. El ingeniero Schaller trabaja en la empresa SIAT con redes industriales.

Uno puede estar tentado a pensar que en la profesión del electrónico, las redes de datos no son importantes, pero hoy en día, el electrónico en la planta no es solo aquel dedicado al instrumental o al hardware, sino que es el electrónico el que tiene la responsabilidad de mantener la programación de sistemas SCADAs (Supervisory Control And Data Acquisition) y RTOS (Real Time Operating System), los cuales requieren de forma mandatoria utilizar una red.

El electrónico que se encarga del software, nos dice el ingeniero Schaller, debe conocer sobre redes LAN, no al punto de diseñar una red, optimizarla, o manejar redundancias, pero si tener a mano las herramientas para diagnosticar en caso de algún problema.

¿Que conceptos debe manejar entonces el electrónico?

El electrónico debe conocer de modelo OSI, de cableados, de direccionamiento, enrutamiento y firewall básicamente, de esta manera, podrá valerse de sus conocimientos para identificar un problema de conectividad en lugar de sospechar de la lógica del SCADA o del sistema que esté desarrollando

Capítulo 2

Información Previa Requerida

RESUMEN: Veremos al recorrer este capítulo, un diagrama formal del diseño de la red, definiendo su topología y sus segmentos IP, veremos requerimientos y algunos conceptos básicos.

2.1. Conceptos Básicos y Generales

2.1.1. ¿Qué es una red informática?

En informática, una red es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información, servicios, etc. Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos. Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios.

2.1.2. ¿Qué es un servidor?

En informática, un servidor es un ordenador que, formando parte de una red, provee servicios a otros ordenadores denominados clientes.

2.1.3. Tipos de redes según el tamaño

Se distinguen diferentes tipos de redes según su tamaño, su velocidad de transferencia de datos y su alcance. Generalmente se dice que existen tres categorías de redes:

LAN (Red de área local). LAN significa Red de área local. Un conjunto de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica.

MAN (Red de área metropolitana): conecta diversas LAN cercanas geográficamente entre sí a alta velocidad. Por lo tanto, una MAN permite que dos nodos remotos se comuniquen como si fueran parte de la misma red de área local. Una MAN está compuesta por conmutadores o routers conectados entre sí mediante conexiones de alta velocidad.

WAN (Red de área mundial). Conecta múltiples LAN entre sí a través de grandes distancias geográficas. La velocidad disponible en una WAN varía según el costo de las conexiones y puede ser baja. Las WAN funcionan con routers, que pueden elegir la ruta más apropiada para que los datos lleguen a un nodo de la red. La WAN más conocida es Internet.

2.1.4. ¿Como elegir direcciones IP para una red?

Una parte importante del diseño de la red, es el dimensionamiento (en cantidad de equipos) de la misma, en base a su dimensión serán las direcciones que se elijan. Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/-conexión) de un dispositivo dentro de una red.

Las direcciones IP [1] se expresan por un número binario de 32 bits permitiendo un espacio de direcciones de 4.294.967.296 (2^32) direcciones posibles.

Las direcciones IP se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el rango de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores

[1] En este documento hablaremos siempre de IPv4, si bien en el mundo ya se está utilizando IPv6 para los direccionamientos públicos, entendemos que a los fines de este proyecto (dar al electrónico los conceptos básicos de redes) no agrega valor en ninguna circunstancia. Si es deseo del lector conocer este campo, recomendamos la lectura de: http://www.consulintel.es/html/ForoIPv6/Documentos/Tutorial%20%de%20IPv6.pdf

decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255]. En la expresión de direcciones IP en decimal se separa cada octeto por un carácter único ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255, salvo algunas excepciones.

En una dirección IP, se dividen dos partes importantes, una parte de la dirección define la red y otra parte define el host (el equipo poseedor de esa dirección), esto se ve definido por la máscara de red.

2.1.4.1. Máscara de Subred

La máscara de red es una combinación de bits que sirve para delimitar el ámbito de una red de computadoras. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la que corresponde al host. Básicamente, mediante la máscara de red una computadora podrá saber si debe enviar los datos dentro o fuera de las redes.

A nivel técnico, la máscara de subred es, una vez mas, una etiqueta binaria de 32 bits que define, de los bits de la dirección IP, que porción es la que define la red y que porción está libre para utilizarse por hosts, veámoslo ejemplificado:

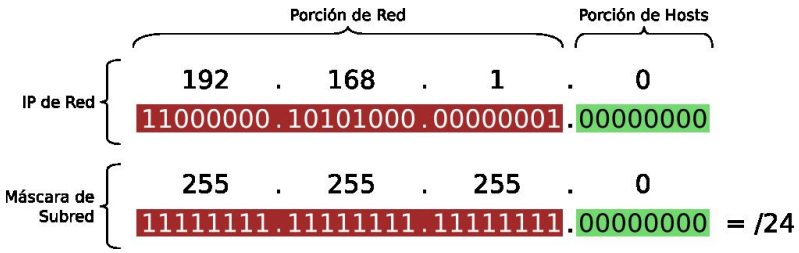

Figura 2.1

Es decir, aquellos bits que valen "1" en la máscara son bits fijos de la dirección de tal manera que definen la red.

2.1.4.2. Clases y Subredes

En 1981 el direccionamiento internet fue revisado y se introdujo la arquitectura de clases (Classful Network Architecture). En esta arquitectura hay tres clases de direcciones IP que una organización puede recibir de parte de la

Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C.

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es $2^{24} - 2$ (se excluyen la dirección reservada para broadcast y de red que se explicarán mas adelante), es decir, 16.777.214 hosts.

- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es $2^{16} - 2$, o 65.534 hosts.

- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es $2^{8} - 2$, ó 254 hosts.

Como ya conocemos el concepto de máscara, podemos decir y entender que:

CLASE	MÁSCARA DE SUBRED
Clase A	255.0.0.0
Clase B	255.255.0.0
Clase C	255.255.255.0

Tabla 2.1: Las clases y sus máscaras de subred

Sin embargo, la existencia de estas clases, no limita la existencia de otras máscaras que no sean las listadas, por el contrario, podemos partir esas clases en subredes, por ejemplo, si soy poseedor de un segmento de red
131.18.0.0/16 (Clase B) pero quiero aislar redes mas pequeñas dentro de ella, puedo hacerlo, podría por ejemplo generar dos subredes (práctica conocida incluso en español como subnetting) reduciendo su capacidad a la mitad de hosts (en realidad no es exactamente la mitad porque se duplican las direcciones reservadas para ip de red y de broadcast. Véase 2.1.4.3), es decir, quedarían las redes 131.18.0.0/17 y 131.18.128.0/17, con capacidad 32766 hosts cada una. En general es:

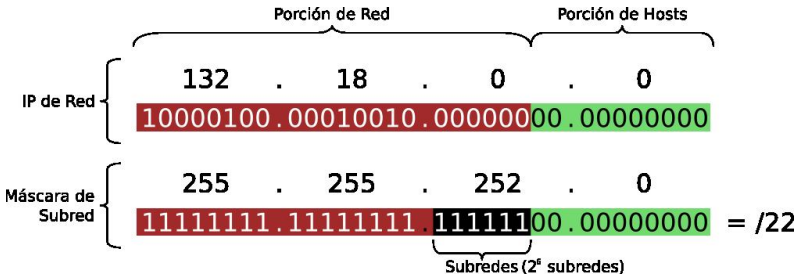

Figura 2.2

Para no ahondar en este tema, que requiere mucha práctica, recomendamos hacer ejercicios y proponemos utilizar la herramienta disponible en http://www.subnet-calculator.com/ para chequear resultados[2].

2.1.4.3. Direcciones Reservadas

- La dirección 0.0.0.0 es reservada por la IANA para identificación local.
- La dirección que tiene los bits de host iguales a cero sirve para definir la red en la que se ubica. Se denomina dirección de red. En el ejemplo de la figura 2.2 la IP de red es la 132.18.0.0
- La dirección que tiene los bits correspondientes a host iguales a uno, sirve para enviar paquetes a todos los hosts de la red en la que se ubica. Se denomina dirección de broadcast. Siguiendo el mismo ejemplo, la IP de broadcast para la red 131.18.0.0/22 es la 131.18.3.255 (10000100. 00010010. 000000 11.11111111)
- Las direcciones 127.x.x.x se reservan para designar la propia máquina. Se denomina dirección de bucle local o loopback.

2.1.4.4. Direcciones privadas

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT. Las direcciones privadas son:

[2] Para usuarios de GNU/Linux recomendamos el software "gip" para este fin

- Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).

- Clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.

- Clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts). 256 redes clase C contiguas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

2.2. Modelo OSI

El modelo de interconexión de sistemas abiertos, también llamado OSI (en inglés open system interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización en el año 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Figura 2.3: Modelo OSI

Siguiendo el esquema de este modelo se crearon numerosos protocolos. El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo es muy usado en la enseñanza como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones. El modelo especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usa- do como una gran herramienta para la enseñanza de comunicación de redes. Este modelo está dividido en siete capas:

2.2.1. Capa física

Es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información. Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas del medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de dicha conexión).

2.2.2. Capa de enlace de datos

Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso al medio, de la detección de errores y de la distribución ordenada de tramas.

2.2.3. Capa de red

Se encarga de identificar el enrutamiento existente entre una o más redes. Las unidades de información se denominan paquetes, y se pueden clasificar en protocolos enrutables y protocolos de enrutamiento.

Enrutables: viajan con los paquetes (IP, IPX, APPLETALK)

Enrutamiento: permiten seleccionar las rutas (RIP, IGRP, EIGP, OSPF, BGP)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan enrutadores, aunque es más frecuente encontrarlo con el nombre en inglés routers. Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas. En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

2.2.4. Capa de transporte

Capa encargada de efectuar el control de flujo y el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP. Sus protocolos son TCP y UDP; el primero orientado a conexión y el otro sin conexión. Trabajan, por lo tanto, con puertos lógicos y junto con la capa red dan forma a los conocidos como Sockets IP:Puerto (191.16.200.54:80).

2.2.5. Capa de sesión

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

2.2.6. Capa de presentación

El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos. Por lo tanto, podría decirse que esta capa actúa como un traductor.

2.2.7. Capa de aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (Post Office Protocol y SMTP), gestores de bases de datos y servidor de ficheros (FTP), por UDP pueden viajar (DNS y Routing Information Protocol). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

2.3. Modelo TCP/IP

El estándar histórico y técnico de la Internet es el modelo TCP/IP. El Departamento de Defensa de EE.UU. creó el modelo de referencia TCP/IP porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear.

A diferencia de las tecnologías de networking propietarias, el TCP/IP se desarrolló como un estándar abierto. Esto significaba que cualquier persona podía usar el TCP/IP. Esto contribuyó a acelerar el desarrollo de TCP/IP como un estándar.

El modelo TCP/IP tiene las siguientes cuatro capas:

- Capa de aplicación
- Capa de transporte
- Capa de Red
- Capa de acceso a la red

Aunque algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta. Lo más notable es que la capa de aplicación posee funciones diferentes en cada modelo.

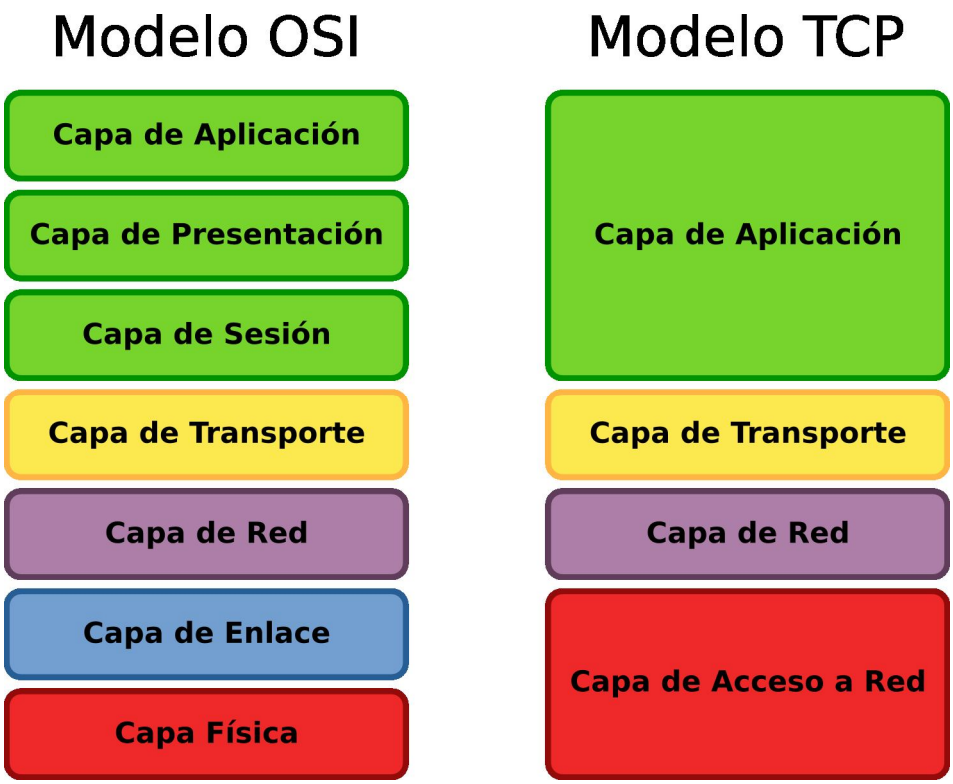

Figura 2.4: Modelo TCP/IP

Los diseñadores de TCP/IP sintieron que la capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI. Crearon una capa de aplicación que maneja aspectos de representación, codificación y control de diálogo.

Parte II

Documentación Relevante

Aquí presentamos la información técnica requerida y utilizada durante el desarrollo del proyecto

Capítulo 3

Virtualización

En Informática, virtualización se refiere a la abstracción de los recursos de una computadora, llamada Hipervisor o VMM (Virtual Machine Monitor) que crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest), siendo un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución.

Esta capa de software (VMM) maneja, gestiona y arbitra los cuatro recursos principales de una computadora (CPU, Memoria, Red, Almacenamiento) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. De modo que nos permite tener varios ordenadores virtuales ejecutándose sobre el mismo ordenador físico.

La máquina virtual en general es un sistema operativo completo que corre como si estuviera instalado en una plataforma de hardware autónoma. Típicamente muchas máquinas virtuales son ejectadas en un mismo Hipervisor

Entre las ventajas de la utilización de la tecnología de virtualización se puede mencionar:

- Rápida incorporación de nuevos recursos para los servidores virtualizados.
- Reducción de los costes de espacio y consumo necesario de forma proporcional al índice de consolidación logrado (Estimación media 10:1).
- Administración global centralizada y simplificada.

- Nos permite gestionar nuestro CPD como un pool de recursos o agrupación de toda la capacidad de procesamiento, memoria, red y almacenamiento disponible en nuestra infraestructura
- Mejora en los procesos de clonación y copia de sistemas: Mayor facilidad para la creación de entornos de test que permiten poner en marcha nuevas aplicaciones sin impactar a la producción, agilizando el proceso de las pruebas.
- Aislamiento: un fallo general de sistema de una máquina virtual no afecta al resto de máquinas virtuales. Mejora de TCO y ROI.
- No sólo aporta el beneficio directo en la reducción del hardware necesario, sino también los costes asociados.
- Reduce los tiempos de parada.
- Migración en caliente de máquinas virtuales (sin pérdida de servicio) de un servidor físico a otro, eliminando la necesidad de paradas planificadas por mantenimiento de los servidores físicos.
- Balanceo dinámico de máquinas virtuales entre los servidores físicos que componen el pool de recursos, garantizando que cada máquina virtual ejecute en el servidor físico más adecuado y proporcionando un consumo de recursos homogéneo y óptimo en toda la infraestructura.

La virtualización se ha convertido en nuestros días en una herramienta indispensable en casi todos los ámbitos. Tanto en el mundo empresarial como para los usuarios domésticos la virtualización lo está invadiendo todo porque aporta numerosas ventajas como las descriptas anteriormente.

Esta tecnología puede clasificarse en dos grandes grupos: Virtualización de primer nivel y Virtualización de segundo nivel.

De Primer Nivel

El software de virtualización de tipo 1, o de primer nivel, se instala directamente sobre el equipo haciendo éste las funciones tanto de sistema operativo como las de virtualización.

Este método de virtualización lo utilizan sobre todo las empresas que pueden disponer de uno o varios servidores dedicados en exclusiva a la virtualización de sistemas.

VMWARE ESXI, por ejemplo, es una plataforma de virtualización de tipo 1. Éste tipo de sistemas se instalan en servidores sin

ningún otro sistema operativo. Él mismo lleva un núcleo de Linux optimizado para las tareas de virtualización y requiere que el hardware sea compatible, principalmente que el microprocesador posea el set de instrucciones de virtualización (VT-x para el caso de Intel)

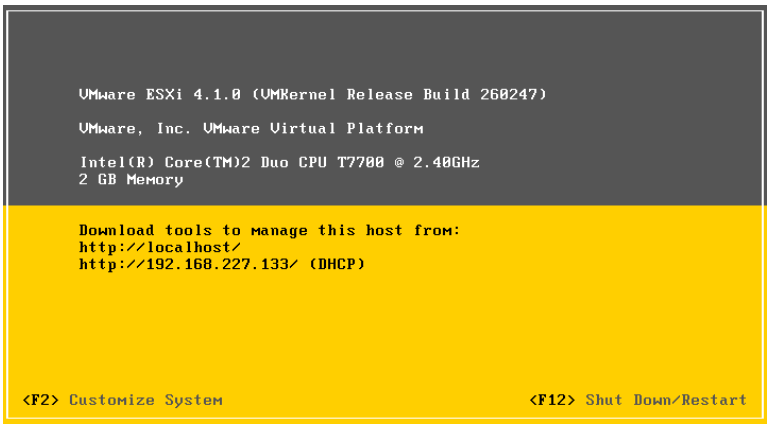

Figura 3.1: VMware ESXi

VMware ESXi requiere además del servidor donde estará instalado, un cliente para administrarlo (como se nota en la captura de pantalla del servidor que se muestra en la imagen anterior)

De Segundo Nivel

El software de virtualización de tipo 2, o de segundo nivel, se caracteriza porque debe ser instalado en un equipo que cuente con un sistema operativo previo (como Ubuntu, Fedora, Microsoft Windows o Mac OS X).

Para un usuario doméstico éste es el método de virtualización apropiado.

En este grupo encontraremos una amplia variedad de productos, entre ellos se destacan ORACLE xVM VIRTUALBOX, VMWARE WORKSTATION, VMWARE SERVER, KVM, MICROSOFT VIRTUAL PC, entre otros.

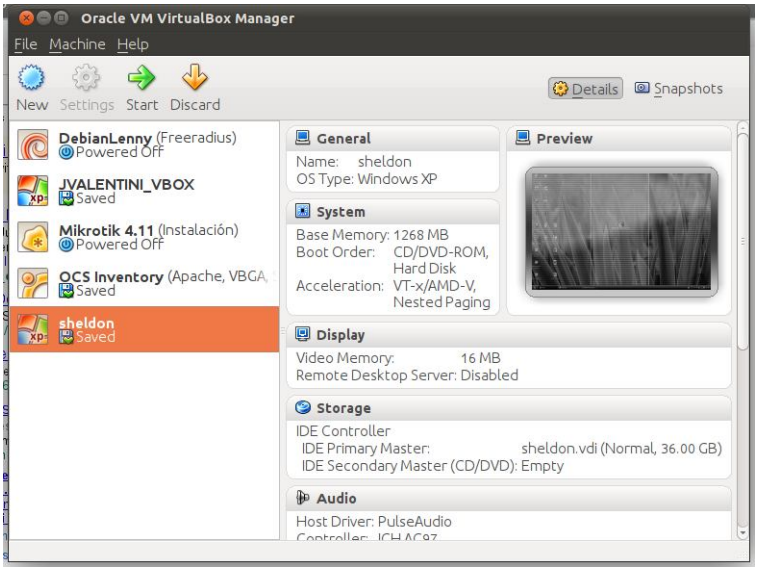

Figura 3.2: Oracle xVM VirtualBox

En la imagen se ve una captura de VirtualBox, este es quizás uno de los hipervisores mas utilizados en la virtualización para usuarios de escritorio, ya que es gratuito, multiplataforma y muy sencillo de utilizar, además posee una interfaz por línea de comandos, por lo que permite que las máquinas virtuales corran en segundo plano, y sin siquiera verlas, ofrezcan los servicios para los que fueron configuradas.

Capítulo 4

Redes de Datos

RESUMEN: Este capítulo es quizás el que abarca más conceptos y más información técnica, en el, el lector encontrará descriptos muchos de los aspectos que luego se verán puestos en práctica

4.1. Ethernet

La mayor parte del tráfico en Internet se origina y termina en conexiones de Ethernet. Desde su comienzo en la década de 1970, Ethernet ha evolucionado para satisfacer la creciente demanda de LAN de alta velocidad. En el momento en que aparece un nuevo medio, como la fibra óptica, Ethernet se adapta para sacar ventaja de un ancho de banda superior y de un menor índice de errores que la fibra ofrece. Ahora, el mismo protocolo que transportaba datos a 3 Mbps en 1973 transporta datos a 10 Gbps.

La idea original de Ethernet nació del problema de permitir que dos o más host utilizaran el mismo medio y evitar que las señales interfirieran entre sí. El problema de acceso por varios usuarios a un medio compartido se estudió a principios de los 70 en la Universidad de Hawai. Se desarrolló un sistema llamado Alohanet para permitir que varias estaciones de las Islas de Hawai tuvieran acceso estructurado a la banda de radiofrecuencia compartida en la atmósfera. Más tarde, este trabajo sentó las bases para el método de acceso a Ethernet conocido como CSMACD.

CSMACD significa que se utiliza un medio de acceso múltiple y que la estación que desea emitir previamente escucha el canal.

Una vez comenzado emitir, no para hasta terminar de enviar la trama completa. Si se produjera alguna colisión (que dos tramas de distinta estación fueran enviadas a la vez en el canal) ambas tramas serán incompresibles para las otras estaciones y la transmisión fracasaría.

Finalmente CSMACD supone una mejora sobre CSMA, pues la estación está a la escucha a la vez que emite, de forma que si detecta que se produce una colisión, detiene inmediatamente la transmisión.

El éxito de Ethernet se debe a los siguientes factores:

- Sencillez y facilidad de mantenimiento.
- Capacidad para incorporar nuevas tecnologías.
- Confiabilidad
- Bajo costo de instalación y de actualización.

En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con el modelo OSI de la Organización Internacional de Estándares (ISO). Por eso, el estándar IEEE 802.3 debía cubrir las necesidades de la Capa 1 y de las porciones inferiores de la Capa 2 del modelo OSI. Como resultado, ciertas pequeñas modificaciones al estándar original de Ethernet se efectuaron en el 802.3.

4.1.1. Ethernet en el Modelo OSI

Ethernet opera en dos áreas del modelo OSI, la mitad inferior de la capa de enlace de datos, conocida como subcapa MAC y la capa física.

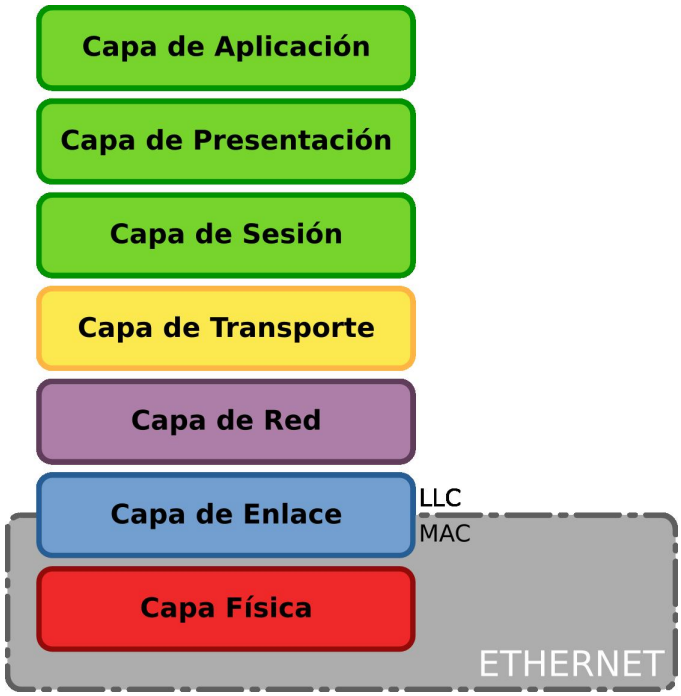

Figura 4.1: Las capas de trabajo de Ethernet

4.2. Wi-Fi

Wi-Fi es el nombre que se le da a una red de datos inalámbrica en particular, compatible con una gran variedad de dispositivos y usualmente utilizada para acceder a internet (Tal es así, que el solo hecho de que exista una red Wi-Fi, hace suponer al usuario que conectándose a ella podrá acceder a internet).

Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11 (y sus derivados). La especificación IEEE 802.11 (ISO/IEC 8802-11) es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). A los dispositivos certificados por la Wi-Fi Alliance se les permite usar este logotipo:

Figura 4.2

Como en el caso de las redes cableadas, la IEEE es la principal generadora de estándares para las redes inalámbricas. Los estándares han sido creados en el marco de las reglamentaciones creadas por el FCC:

- 802.11
- 802.11b
- 802.11g
- 802.11a

La tecnología clave que contiene el estándar 802.11 es el DSSS, este estándar ha caído en desuso por su baja velocidad de transferencia de datos (un máximo de 2Mb). El siguiente estándar aprobado fue el 802.11b, que aumentó las capacidades de transmisión a 11 Mbps.

Los dispositivos de 802.11b logran un mayor índice de tasa de transferencia de datos ya que utilizan una técnica de codificación diferente a la del 802.11, permitiendo la transferencia de una mayor cantidad de datos en la misma cantidad de tiempo.

802.11a abarca los dispositivos WLAN que operan en la banda de transmisión de 5 GHz. El uso del rango de 5 GHz no permite la interoperabilidad de los dispositivos 802.11b ya que éstos operan dentro de los 2,4 GHz. 802.11a puede proporcionar una tasa de transferencia de datos de 54 Mbps y con una tecnología propietaria que se conoce como "duplicación de la velocidad" ha alcanzado los 108 Mbps. En las redes de producción, la velocidad estándar es de 20-26 Mbps.

802.11g tiene la capacidad de ofrecer la misma tasa de transferencia que 802.11a pero con compatibilidad retrospectiva para los dispositivos 802.11b.

En resumen, las redes Wi-Fi a las que estamos más habituados son aquellas que cumplen con el estándar 802.11b y 802.11g

4.2.1. Topología

Si bien una red Wi-Fi se puede establecer entre dos interfaces de red como las que se muestran en la figura 4.3(topología que se conoce como Ad-Hoc), se suele instalar un punto de acceso (Normalmente llamado por el acrónimo de sus siglas en inglés: AP. Véase la sección 4.4.5 en la página 49) para

que actúe como hub central para el modo de infraestructura de la WLAN. El AP (Figura 4.4) se conecta mediante cableado a la LAN a fin de proporcionar acceso a Internet y conectividad a la red cableada. Los AP están equipados con antenas y brindan conectividad inalámbrica a un área específica que recibe el nombre de celda. Según la composición estructural del lugar donde se instaló el AP y del tamaño y ganancia de las antenas, el tamaño de la celda puede variar enormemente. Por lo general, el alcance es de 50 a 150 metros.

Figura 4.3: Interfaces de red WLAN

Figura 4.4: Access Point Cisco

4.2.2. Seguridad de Redes Inalámbricas

Hoy en día, casi podríamos asumir que hay un access point en cada hogar, esto también trae aparejado que cada vez mas gente, se interese en configurarlo por si misma. Se sabe que la mayoría de los usuarios hogareños

al llegar a la configuración de la seguridad de red, aturdido por una "sopa de letras" de diferentes encriptaciones y métodos de autenticación, acaban por dejar sus redes sin ninguna protección. Como se pretende que este documento sirva de guía para un personal técnico no especializado en redes, se quiere comenzar esta sección con un pequeño "diccionario" de todo lo que se puede encontrar en materia de seguridad de redes inalámbricas.

WEP: Wired Equivalent Privacy. Es el antiguo y original método de autenticación y encriptación. Actualmente es fácilmente vulnerado.

WEP 40/128-bit key, WEP 128-bit Passphrase: Ver WEP. La clave wep es de 40 ó 128 bits de longitud, es por eso que muchas veces WEP se encuentra expresado de esa manera.

WPA, WPA1: Wi-Fi Protected Access. La versión inicial de WPA, a veces llamada WPA1, Es esencialmente un nombre comercial para TKIP. TKIP fue elegido como un estándar intermedio ya que podía implementarse en hardware compatible con WEP con solo una actualización de firmware.

WPA2: El nombre comercial de una implementación del estándar 802.11i, incluyendo AES y CCMP.

TKIP: Temporal Key Integrity Protocol. El sistema de encriptación definido para reemplazar a WEP. Muchas características nuevas fueron añadidas para hacer de las claves bajo TKIP mas seguras que en WEP.

AES: Advanced Encryption Standard. Actualmente es el método de encriptación preferido, reemplazando al viejo TKIP. AES se implementa en WPA2/802.11i.

Dynamic WEP (802.1x): Cuando la clave WEP es ingresada por un servicio de administración de claves. WEP por si mismo no soportaba las claves dinámicas, esta característica se agregó con el advenimiento de TKIP y CCMP.

EAP: Extensible Authentication Protocol. Una estructura estándar para la autenticación. EAP provee funciones comunes y un mecanismo de negociación, pero no un método específico de autenticación. Actualmente existen alrededor de 40 métodos diferentes para trabajar con EAP.

802.1x, IEEE8021X: El estándar de IEEE para autenticación en redes.

LEAP, 802.1x EAP (Cisco LEAP): Lightweight Extensible Authentication Protocol. Un método propietario de autenticación a redes inalámbricas desarrollado por Cisco Systems. Soporta WEP dinámico, RADIUS y reautenticación frecuente.

WPA-PSK: WPA-Preshared Key. Se usa una clave compartida, una clave configurada manualmente y administrada manualmente. No es recomendable

para una gran red, tanto por administración como por seguridad, pero en contraparte no requiere ningún tipo de sistema de administración de claves, lo que lo hace ideal para entornos pequeños.

RADIUS: Remote Authentication Dial In User Service. Un protocolo antiguo pero vigente que sirve para centralizar la autenticación y la administración de la autorización. Un servidor RADIUS actúa como servicio remoto para este fin.

WPA Enterprise, WPA2 Enterprise: La marca comercial que agrupa algunas variedades de EAP (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC y EAP-SIM)

WPA-Personal, WPA2-Personal: Equivalente a WPA-PSK.

WPA2-Mixed: Soporta tanto WPA como WPA2 en un mismo access point.

802.11i: un estándar de la IEEE que especifica los mecanismos de seguridad para redes 802.11. 802.11i usa AES e incluye mejoras en la administración de claves, autenticación de usuarios a través de 802.1X y maneja integridad de datos.

CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. Un protocolo de encriptación basado en AES.

WEP es un método de seguridad de red antiguo que todavía está disponible para dispositivos antiguos, pero que ya no se recomienda usar. Cuando se habilita WEP, se configura una clave de seguridad de red. Esta clave cifra la información que un equipo envía a otro a través de la red. Sin embargo, la seguridad WEP es relativamente fácil de vulnerar.

Actualmente no es recomendable usar WEP en ambientes donde la privacidad es importante. WPA o WPA2 son más seguros. Si prueba WPA o WPA2 y no funcionan, se recomienda que actualice su adaptador de red a uno que sea compatible con WPA o WPA2.

WPA cifra la información y también comprueba que la clave de seguridad de red no haya sido modificada. Además, WPA autentica a los usuarios con el fin de garantizar que únicamente los usuarios autorizados puedan tener acceso a la red.

Existen dos tipos de autenticación WPA: WPA y WPA2. WPA se ha diseñado para trabajar con todos los adaptadores de red inalámbrica, pero es posible que no funcione con enrutadores o puntos de acceso antiguos. WPA2 es más seguro que WPA, pero no funcionará con algunos adaptadores de red antiguos. WPA se ha diseñado para utilizarse con un servidor de autenticación

802.1x, que distribuye claves diferentes a cada usuario. Esto se denomina WPA-Enterprise o WPA2-Enterprise. También se puede usar en el modo de clave previamente compartida (PSK), donde cada usuario recibe la misma frase de contraseña. Esto se denomina WPA-Personal o WPA2-Personal.

La autenticación 802.1x puede ayudar a mejorar la seguridad de las redes inalámbricas 802.11 (y de las redes Ethernet con cable). 802.1x utiliza un servidor de autenticación para validar a los usuarios y proporcionar acceso a la red. En las redes inalámbricas, 802.1x puede funcionar con claves WEP (Privacidad equivalente por cable) o WPA (Acceso protegido Wi-Fi). Esta tipo de configuración se suele utilizar al conectarse a una red de área de trabajo.

4.3. Capa de transporte

Las tareas principales de la capa de transporte, la Capa 4 del modelo OSI, son transportar y regular el flujo de información desde el origen hasta el destino, de forma confiable y precisa. El control de extremo a extremo y la confiabilidad se suministran a través de ventanas deslizantes, números de secuencia y acuses de recibo.

El transporte confiable puede lograr lo siguiente:

- Asegurarse de que se acuse recibo de los segmentos entregados
- Realizar la retransmisión de cualquier segmento que no genere acuse de recibo
- Volver a poner los segmentos en su secuencia correcta en el destino
- Evitar y controlar la congestión

Para comprender qué son la confiabilidad y el control de flujo, piense en alguien que estudia un idioma extranjero durante un año y luego visita el país en el que se habla ese idioma. Mientras uno conversa, las palabras se deben repetir para que exista confiabilidad y se debe hablar lentamente de modo que el significado de la conversación no se pierda; esto es lo que se denomina control de flujo.

La capa de transporte brinda servicios de transporte desde el host origen hasta el host destino. Establece una conexión lógica entre los puntos de terminación de la red. Los protocolos de la capa de transporte segmentan y reensamblan los datos mandados por las aplicaciones de capas superiores en

el mismo flujo de datos de capa de transporte. Este flujo de datos de la capa de transporte brinda servicios de transporte de extremo a extremo.

4.3.1. Protocolo para el Control de la Transmisión (TCP)

El Protocolo para el control de la transmisión (TCP) es un protocolo de Capa 4 orientado a conexión que suministra una transmisión de datos full-duplex confiable. TCP forma parte de la pila del protocolo TCP/IP. En un entorno orientado a conexión, se establece una conexión entre ambos extremos antes de que se pueda iniciar la transferencia de información. TCP es responsable por la división de los mensajes en segmentos, reensamblándolos en la estación destino, reenviando cualquier mensaje que no se haya recibido y reensamblando mensajes a partir de los segmentos. TCP suministra un circuito virtual entre las aplicaciones del usuario final.

Los protocolos que usan TCP incluyen FTP, HTTP, SMTP, Telnet, entre otros (Véase la sección 4.5 en la página 55).

4.3.2. Protocolo de Datagrama de Usuario (UDP)

El Protocolo de datagrama de usuario (UDP: User Datagram Protocol) es el protocolo de transporte no orientado a conexión de la pila de protocolo TCP/IP. El UDP es un protocolo simple que intercambia datagramas sin acuse de recibo ni garantía de entrega. El procesamiento de errores y la retransmisión deben ser manejados por protocolos de capa superior.

El UDP no usa ventanas ni acuses de recibo de modo que la confiabilidad, de ser necesario, se suministra a través de protocolos de la capa de aplicación. El UDP está diseñado para aplicaciones que no necesitan ensamblar secuencias de segmentos.

Los protocolos que usan UDP incluyen TFTP, SNMP, DHCP, DNS, entre otros (Véase la sección 4.5 en la página 55).

4.3.3. Números de puerto TCP y UDP

Tanto TCP como UDP utilizan números de puerto (socket) para enviar información a las capas superiores. Los números de puerto se utilizan para mantener un registro de las distintas conversaciones que atraviesan la red al mismo tiempo.

Los programadores del software de aplicación han aceptado usar los números de puerto conocidos que emite la IANA. Cualquier conversación dirigida a la aplicación FTP usa los números de puerto estándar 20 y 21. El puerto 20 se usa para la parte de datos y el puerto 21 se usa para control. A las conversaciones que no involucran ninguna aplicación que tenga un número de puerto bien conocido, se les asignan números de puerto que se seleccionan de forma aleatoria dentro de un rango específico por encima de 1023. Algunos puertos son reservados, tanto en TCP como en UDP, aunque es posible que algunas aplicaciones no estén diseñadas para admitirlos. Los números de puerto tienen los siguientes rangos asignados:

- Los números inferiores a 1024 corresponden a números de puerto bien conocidos.
- Los números superiores a 1024 son números de puerto asignados de forma dinámica.
- Los números de puerto registrados son aquellos números que están registrados para aplicaciones específicas de proveedores. La mayoría de estos números son superiores a 1024.

Los sistemas finales utilizan números de puerto para seleccionar la aplicación adecuada.

4.4. Dispositivos de Red

4.4.1. Hub

Los hubs en realidad son repetidores multipuerto. En muchos casos, la diferencia entre los dos dispositivos radica en el número de puertos que cada uno posee. Mientras que un repetidor[1] convencional tiene sólo dos puertos, un hub por lo general tiene de cuatro a veinticuatro puertos. Los hubs por lo general se utilizan en las redes Ethernet (aunque han caído en desuso), aunque hay otras arquitecturas de red que también los utilizan. El uso de un hub hace que cambie la topología de la red desde un bus lineal, donde cada dispositivo se conecta de forma directa al cable, a una en estrella. En un hub, los datos que llegan a un puerto del hub se transmiten de forma eléctrica a todos los otros puertos conectados al mismo segmento de red, salvo a aquel puerto desde donde enviaron los datos.

[1] No se describió el repetidor ya que es un dispositivo que no hace mas que regenerar la señal repitiéndola. No merece explicación alguna

Los hubs vienen en tres tipos básicos:

Pasivo: Un hub pasivo sirve sólo como punto de conexión física. No manipula o visualiza el tráfico que lo cruza. No amplifica o limpia la señal. Un hub pasivo se utiliza sólo para compartir los medios físicos. En sí, un hub pasivo no requiere energía eléctrica.

Activo: Se debe conectar un hub activo a un tomacorriente porque necesita alimentación para amplificar la señal entrante antes de pasarla a los otros puertos.

Inteligente: A los hubs inteligentes a veces se los denomina "smart hubs". Es- tos dispositivos básicamente funcionan como hubs activos, pero también incluyen un chip microprocesador y capacidades diagnósticas. Los hubs inteligentes son más costosos que los hubs activos, pero resultan muy útiles en el diagnóstico de fallas.

Los dispositivos conectados al hub reciben todo el tráfico que se transporta a través del hub. Cuántos más dispositivos están conectados al hub, mayores son las probabilidades de que haya colisiones. Las colisiones ocurren cuando dos o más estaciones de trabajo envían al mismo tiempo datos a través del cable de la red. Cuando esto ocurre, todos los datos se corrompen. Cada dispositivo conectado al mismo segmento de red se considera un miembro de un dominio de colisión.

Algunas veces los hubs se llaman concentradores, porque los hubs sirven como punto de conexión central para una LAN de Ethernet.

4.4.2. Bridge

A veces, es necesario dividir una LAN grande en segmentos más pequeños que sean más fáciles de manejar. Esto disminuye la cantidad de tráfico en una sola LAN y puede extender el área geográfica más allá de lo que una sola LAN puede admitir. Los dispositivos que se usan para conectar segmentos de redes son los bridges (puentes), switches (conmutadores), routers (entrutadores) y gateways (puertas de enlace). Los switches y los puentes operan en la capa de enlace de datos del modelo de referencia OSI. La función del puente es tomar decisiones inteligentes con respecto a pasar señales o no al segmento siguiente de la red.

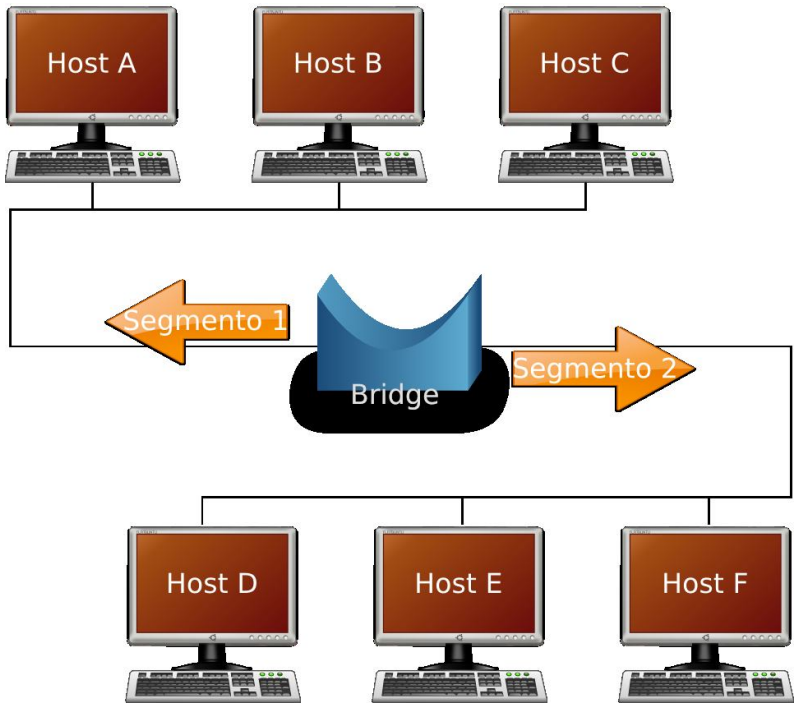

Figura 4.5: Bridge (Puente)

Cuando un puente recibe una trama a través de la red, se busca la dirección MAC destino en la tabla de puenteo para determinar si hay que filtrar, inundar, o copiar la trama en otro segmento. El proceso de decisión tiene lugar de la siguiente forma:

- Si el dispositivo destino se encuentra en el mismo segmento que la trama, el puente impide que la trama vaya a otros segmentos. Este proceso se conoce como filtrado.

- Si el dispositivo destino está en un segmento distinto, el puente envía la trama hasta el segmento apropiado.

- Si el puente desconoce la dirección destino, el puente envía la trama a todos los segmentos excepto aquel en el cual se recibió. Este proceso se conoce como inundación.

- Si se ubica de forma estratégica, un puente puede mejorar el rendimiento de la red de manera notoria.

4.4.3. Switch

Un switch se describe a veces como un puente multipuerto. Mientras que un puente típico puede tener sólo dos puertos que enlacen dos segmentos de red, el switch puede tener varios puertos, según la cantidad de segmentos de red que sea necesario conectar. Al igual que los puentes, los switches aprenden determinada información sobre los paquetes de datos que se reciben de los distintos equipos de la red. Los switches utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están mandando de un host a otro de la red.

Aunque hay algunas similitudes entre los dos, un switch es un dispositivo más sofisticado que un puente. Un puente determina si se debe enviar una trama al otro segmento de red, basándose en la dirección MAC destino. Un switch tiene muchos puertos con muchos segmentos de red conectados a ellos. El switch elige el puerto al cual el dispositivo o estación de trabajo destino está conectado. Los switches Ethernet están llegando a ser soluciones para conectividad de uso difundido porque, al igual que los bridges, mejoran el rendimiento de la red al mejorar la velocidad y el ancho de banda.

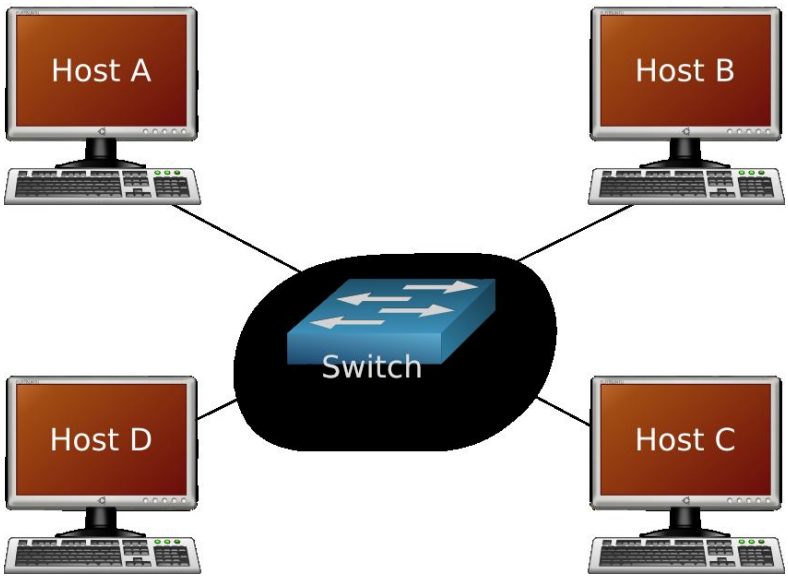

Figura 4.6: Switch (Conmutador)

La conmutación es una tecnología que alivia la congestión en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los switches pueden remplazar a los hubs con facilidad debido a que ellos funcionan con las infraestructuras de cableado existentes. Esto mejora el rendimiento

con un mínimo de intrusión en la red ya existente.

Actualmente en la comunicación de datos, todos los equipos de conmutación realizan dos operaciones básicas: La primera operación se llama conmutación de las tramas de datos. La conmutación de las tramas de datos es el procedimiento mediante el cual una trama se recibe en un medio de entrada y luego se transmite a un medio de salida. El segundo es el mantenimiento de operaciones de conmutación cuando los switch crean y mantienen tablas de conmutación y buscan loops. Los switches operan a velocidades mucho más altas que los puentes y pueden admitir nuevas funcionalidades como, por ejemplo, las LAN virtuales (VLANs).

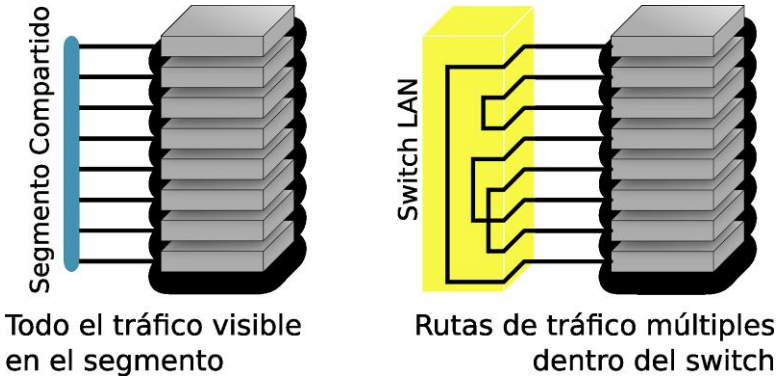

Figura 4.7: Rutas dedicadas entre hosts en un Switch

Un switch Ethernet ofrece muchas ventajas. Un beneficio es que un switch para Ethernet permite que varios usuarios puedan comunicarse en paralelo usando circuitos virtuales y segmentos de red dedicados en un entorno virtualmente sin colisiones (Figura 4.7). Esto aumenta al máximo el ancho de banda disponible en el medio compartido. Otra de las ventajas es que desplazarse a un entorno de LAN conmutado es muy económico ya que el hardware y el cableado se pueden volver a utilizar.

4.4.4. Router

Un router —anglicismo a veces traducido en español como encaminador o enrutador— es un dispositivo de hardware usado para la interconexión de redes informáticas[2] que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar. Opera en la capa tres del modelo OSI

[2]Recuerde lo visto en la sección 2.1.4 acerca de subredes. Página 18

Los routers son los responsables, por ejemplo, de enrutar paquetes de datos desde su origen hasta su destino en la LAN, y de proveer conectividad a la WAN. Dentro de un entorno de LAN, el router contiene broadcasts, brinda servicios locales de resolución de direcciones, tal como ARP, y puede segmentar la red utilizando una estructura de subred. Para brindar estos servicios, el router debe conectarse a la LAN y a la WAN.

4.4.5. Access Point

El Access Point o AP, es aquel dispositivo con la capacidad de actuar como un switch para el caso de redes inalámbricas (Vea la sección 4.2.1). Cuando se activa un cliente inalámbrico dentro de la LAN, la red comenzará a "escuchar" para ver si hay un dispositivo compatible con el cual "asociarse". Esto se conoce como "escaneo". El escaneo activo hace que se envíe un pedido de sondeo desde el nodo inalámbrico que busca conectarse a la red. Este pedido de sondeo incluirá el Identificador del Servicio (SSID) de la red a la que se desea conectar. Cuando se encuentra un AP con el mismo SSID, el AP emite una respuesta de sondeo y se completan los pasos de autenticación y asociación.

Para brindar servicio a áreas más extensas, es posible instalar múltiples puntos de acceso con cierto grado de superposición. Esta superposición permite pasar de una celda a otra (roaming). Esto es muy parecido a los servicios que brindan las empresas de teléfonos celulares. La superposición, en redes con múltiples puntos de acceso, es fundamental para permitir el movimiento de los dispositivos dentro de la WLAN. Aunque los estándares del IEEE no determinan nada al respecto, es aconsejable una superposición de entre un 20 y un 30 %. Este índice de superposición permitirá el roaming entre las celdas y así la actividad de desconexión y reconexión no tendrá interrupciones.

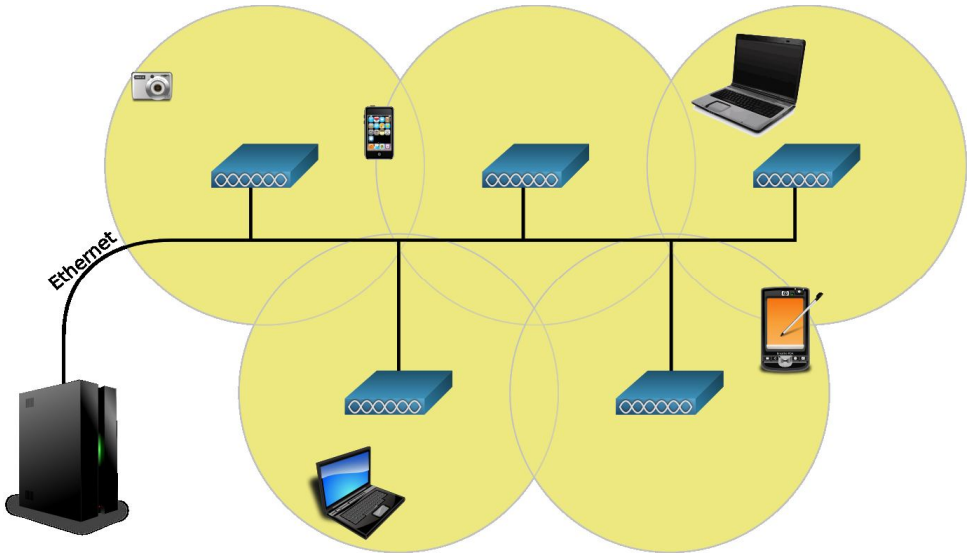

Figura 4.8: Infraestructura de APs superpuestos para Roaming

4.4.6. Firewall

Un cortafuegos (comúnmente llamado firewall incluso en lenguas hispanoparlantes) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir o denegar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de reglas y otros criterios.

Los firewalls pueden ser implementados en hardware o software, o una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet. Todos los mensajes que entren o salgan de la intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada Zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior (Véase la sección 6).

4.4.6.1. Primera Generación: Filtrado de Paquetes

El primer documento publicado para la tecnología firewall data de 1988, cuando un equipo de ingenieros desarrolló los sistemas de filtro conocidos como firewall de filtrado de paquetes. Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet.

El filtrado de paquetes actúa mediante la inspección de los paquetes (que representan la unidad básica de transferencia de datos entre ordenadores en Internet). Si un paquete coincide con el conjunto de reglas del filtro, el paquete se reducirá (descarte silencioso) o será rechazado (desprendiéndose de él y enviando una respuesta de error al emisor). Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico. En su lugar, se filtra cada paquete basándose únicamente en la información contenida en el paquete en sí mismo.

4.4.6.2. Segunda generación: Firewall de estado

Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, desarrollaron la segunda generación de servidores de seguridad. Esta segunda generación cortafuegos tiene en cuenta además la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes (Stateful Firewall), ya que mantiene registros de todas las conexiones que pasan por el cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

4.4.6.3. Tercera generación - Firewall de aplicación

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se abrió paso a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un firewall de capa 7 es mucho más seguro y fiable cuando se compara con uno de filtrado de paquetes, ya que repercute en las siete capas

del modelo OSI. En esencia es similar a un cortafuegos de filtrado de paquetes, con la diferencia de que también podemos filtrar el contenido del paquete.

Un cortafuegos de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, HTTP y TFTP, entre otros. Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear esa palabra en particular. No obstante, los firewalls de aplicación resultan más lentos que los de estado.

4.4.7. Representación Gráfica

Para esquemas de red suelen usarse los estándares de CISCO, es por eso que en este documento también los utilizaremos. Si bien durante este capítulo se fueron incluyendo de manera implícita, vamos a darle su definición formal.

4.4.7.1. Hub

Ya explicado en la sección 4.4.1

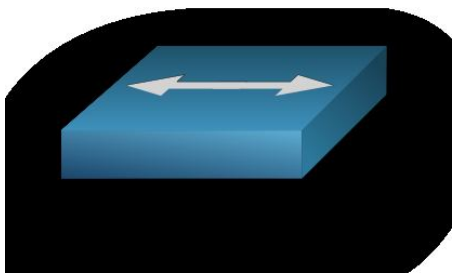

Figura 4.9: Hub

4.4.7.2. Bridge

Ya explicado en la sección 4.4.2

Figura 4.10: Bridge

4.4.7.3. Switch

Ya explicado en la sección 4.4.3

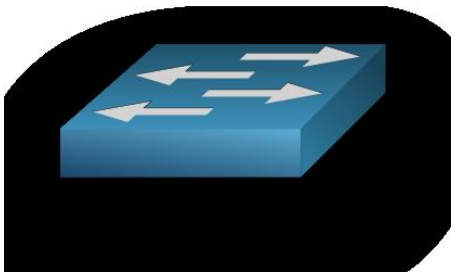

Figura 4.11: Switch

4.4.7.4. Access Point

Ya explicado en la sección 4.4.5

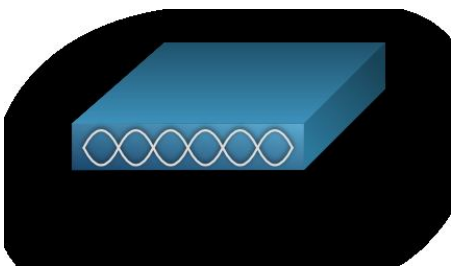

Figura 4.12: Access Point

4.4.7.5. Router

Ya explicado en la sección 4.4.4

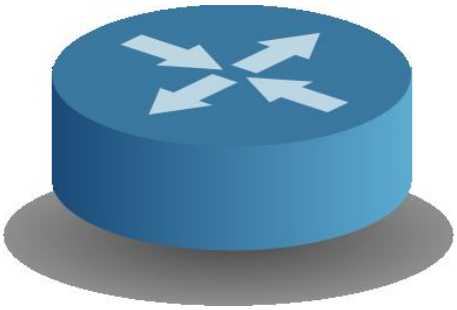

Figura 4.13: Router

4.4.7.6. Firewall

Ya explicado en la sección 4.4.6

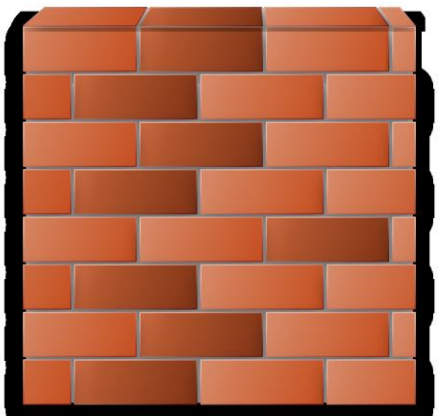

Figura 4.14: Firewall

4.4.7.7. Router-Firewall

Si bien no se ha explicado, considérese que muchas veces, router y firewall están embebidos en el mismo dispositivo. En ese caso se simboliza:

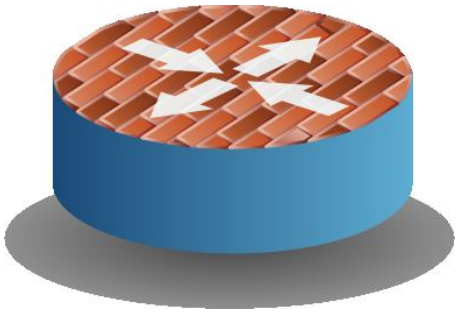

Figura 4.15: Router Firewall

4.5. Servicios en Capa de Aplicación

Cuando se diseñó el modelo TCP/IP, las capas de sesión y de presentación del modelo OSI se agruparon en la capa de aplicación del modelo TCP. Esto significa que los aspectos de representación, codificación y control de diálogo se administran en la capa de aplicación en lugar de hacerlo en las capas inferiores individuales, como sucede en el modelo OSI. Este diseño garantiza que el modelo TCP/IP brinda la máxima flexibilidad, en la capa de aplicación, para los desarrolladores de software.

Los protocolos TCP/IP que admiten transferencia de archivos, correo electrónico y conexión remota probablemente sean los más familiares para los usuarios de la Internet. Estos incluyen, entre otros:

- Servicio de denominación de dominios (DNS)
- Protocolo de transferencia de archivos (FTP)
- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Protocolo simple de administración de red (SNMP)

4.5.1. DNS

La Internet está basada en un esquema de direccionamiento jerárquico. Este esquema permite que el enrutamiento se base en clases de direcciones en lugar de basarse en direcciones individuales. El problema que esto crea para el

usuario es la asociación de la dirección correcta con el sitio de Internet. Es muy fácil olvidarse cuál es la dirección IP de un sitio en particular dado que no hay ningún elemento que permita asociar el contenido del sitio con su dirección. Imaginemos lo difícil que sería recordar direcciones IP de decenas, cientos o incluso miles de sitios de Internet.

Se desarrolló un sistema de denominación de dominio para poder asociar el contenido del sitio con su dirección. El Sistema de denominación de dominios (DNS: Domain Name System) es un sistema utilizado en Internet para convertir los nombres de los dominios y de sus nodos de red publicados abiertamente en direcciones IP. Un dominio es un grupo de computadores asociados, ya sea por su ubicación geográfica o por el tipo de actividad comercial que comparten. Un nombre de dominio es una cadena de caracteres, números o ambos. Por lo general, un nombre o una abreviatura que representan la dirección numérica de un sitio de Internet conforma el nombre de dominio. Existen más de 200 dominios de primer nivel en la Internet, por ejemplo:

.us: Estados Unidos de Norteamérica

.uk: Reino Unido

También existen nombres genéricos, por ejemplo:

.edu: sitios educacionales

.com: sitios comerciales

.gov: sitios gubernamentales

.org: sitios sin fines de lucro

.net: servicio de red

4.5.2. FTP

FTP es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten FTP. El propósito principal de FTP es transferir archivos desde un computador hacia otro copiando y moviendo archivos desde los servidores hacia los clientes, y desde los clientes hacia los servidores. Cuando los archivos se copian de un servidor, FTP primero establece una conexión de control entre el cliente y el servidor. Luego se establece una segunda conexión, que es un enlace entre los computadores a través del cual se transfieren los datos. La transferencia de datos se puede realizar en modo ASCII

o en modo binario. Estos modos determinan la codificación que se usa para el archivo de datos que, en el modelo OSI, es una tarea de la capa de presentación. Cuando termina la transferencia de archivos, la conexión de datos se termina automáticamente. Una vez que se ha completado toda la sesión para copiar y trasladar archivos, el vínculo de comandos se cierra cuando el usuario se desconecta y finaliza la sesión.

TFTP es un servicio no orientado a conexión que usa el Protocolo de datagramas del usuario (UDP). TFTP se usa en el router para transferir archivos de configuración e imágenes de Cisco IOS y para transferir archivos entre sistemas que admiten TFTP. TFTP está diseñado para ser pequeño y fácil de implementar. Por lo tanto, carece de la mayoría de las características de FTP. TFTP puede leer o escribir archivos desde o hacia un servidor remoto pero no puede listar los directorios y no tiene manera de proporcionar autenticación de usuario. Es útil en algunas LAN porque opera más rápidamente que FTP y, en un entorno estable, funciona de forma confiable.

4.5.3. HTTP

El Protocolo de transferencia de hipertexto (http: Hipertext Transfer Protocol) funciona con la World Wide Web, que es la parte de crecimiento más rápido y más utilizada de Internet. Una de las principales razones de este crecimiento sorprendente de la Web es la facilidad con la que permite acceder a la información. Un navegador de Web es una aplicación cliente/servidor, lo que significa que requiere que haya tanto un componente de cliente como de servidor para que funcione. Un navegador de Web presenta datos en formatos multimediales en las páginas Web que usan texto, gráficos, sonido y vídeo. Las páginas Web se crean con un lenguaje de formato denominado Lenguaje de etiquetas por hipertexto (HTML: Hypertext Markup Language). HTML dirige a un navegador de Web en una página Web en particular para crear el aspecto de la página de forma específica. Además, HTML especifica la colocación del texto, los archivos y objetos que se deben transferir desde el servidor de Web al navegador de Web.

Los hipervínculos hacen que la World Wide Web sea fácil de navegar. Un hipervínculo es un objeto, una frase o una imagen en una página Web. Cuando se hace clic en el hipervínculo, transfiere el navegador a otra página Web. La página Web a menudo contiene oculta dentro de su descripción HTML, una ubicación de dirección que se denomina Localizador de Recursos Uniforme (URL: Uniform Resource Locator). En el URL http://www.frsn.utn.edu.ar/tecnicas3, los caracteres "http://"le indican al navegador cuál es el protocolo que debe utilizar. La segunda parte, "www", es el nombre de host o nombre de una máquina determinada con una dirección IP determinada. La última parte identifica la

carpeta específica que contiene la página web por defecto en el servidor.

HTTP://	WWW.	FRSN.UTN.EDU.AR	/TECNICAS3
Le indica al navegador que tipo de protocolo se debe usar	Identifica el nombre de host	El dominio o entidad del sitio	La carpeta donde se encuentra la web en el servidor

Tabla 4.1: Partes de una dirección

Un navegador de Web generalmente se abre en una página de inicio o "home"(de presentación). El URL de la página de presentación ya se ha almacenado en el área de configuración del navegador de Web y se puede modificar en cualquier momento. Desde la página de inicio, haga clic en uno de los hipervínculos de la página Web o escriba un URL en la barra de dirección del navegador. El navegador de Web examina el protocolo para determinar si es necesario abrir otro programa y, a continuación, emplea DNS para determinar la dirección IP del servidor de Web. Luego, las capas de transporte, de red, de enlace de datos y física trabajan de forma conjunta para iniciar la sesión con el servidor Web. Los datos transferidos al servidor HTTP contienen el nombre de carpeta de la ubicación de la página Web. Los datos también pueden contener un nombre de archivo específico para una página HTML. Si no se suministra ningún nombre, se usa el nombre que se especifica por defecto en la configuración en el servidor.

El servidor responde a la petición enviando todos los archivos de texto, audio, vídeo y de gráficos, como lo especifican las instrucciones de HTML, al cliente de Web. El navegador del cliente reensambla todos los archivos para crear una vista de la página Web y luego termina la sesión. Si se hace clic en otra página ubicada en el mismo servidor o en un servidor distinto, el proceso vuelve a empezar.

4.5.4. SMTP

Los servidores de correo electrónico se comunican entre sí usando el Protocolo simple de transferencia de correo (SMTP). El protocolo SMTP transporta mensajes de correo electrónico en formato ASCII usando TCP.

Cuando un servidor de correo recibe un mensaje destinado a un cliente local, guarda ese mensaje y espera que el cliente recoja el correo.

Hay varias maneras en que los clientes de correo pueden recoger su correo. Pueden usar programas que acceden directamente a los archivos del servidor de correo o pueden recoger el correo usando uno de los diversos protocolos de red. Los protocolos de cliente de correo más populares son POP3 e IMAP4, ambos de los cuales usan TCP para transportar datos. Aunque los clientes de correo usan estos protocolos especiales para recoger el correo, casi siempre usan SMTP para enviar correo. Dado que se usan dos protocolos distintos y, posiblemente, dos servidores distintos para enviar y recibir correo, es posible que los clientes de correo ejecuten una tarea y no la otra. Por lo tanto, generalmente es una buena idea diagnosticar los problemas de envío de correo electrónico y los problemas de recepción del correo electrónico por separado.

4.5.5. SNMP

El Protocolo simple de administración de red (SNMP: Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. El SNMP permite que los administradores de red administren el rendimiento de la red, detecten y solucionen los problemas de red y planifiquen el crecimiento de la red. El SNMP usa UDP como su protocolo de capa de transporte.

Una red administrada con SNMP está compuesta por los tres componentes clave que se detallan a continuación:

- Sistema de administración de la red (NMS: Network Management System): El NMS ejecuta aplicaciones que monitorean y controlan los dispositivos administrados. La gran mayoría de los recursos de procesamiento y de memoria que se requieren para la administración de red se suministra a través del NMS. Deben existir uno o más NMS en cualquier red administrada.

- Dispositivos administrados: Los dispositivos administrados son nodos de red que contienen un agente SNMP y que residen en un red administrada. Los dispositivos administrados recopilan y guardan información de administración y ponen esta información a disposición de los NMS usando SNMP. Los dispositivos administrados, a veces denominados elementos de red, pueden ser routers, servidores de acceso, switches y puentes, hubs, hosts del computador o impresoras.

- Agentes: Los agentes son módulos del software de administración de red que residen en los dispositivos administrados. Un agente tiene conocimiento local de la información de administración y convierte esa información a un formato compatible con SNMP.

4.6. VPN

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como la Internet. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede.

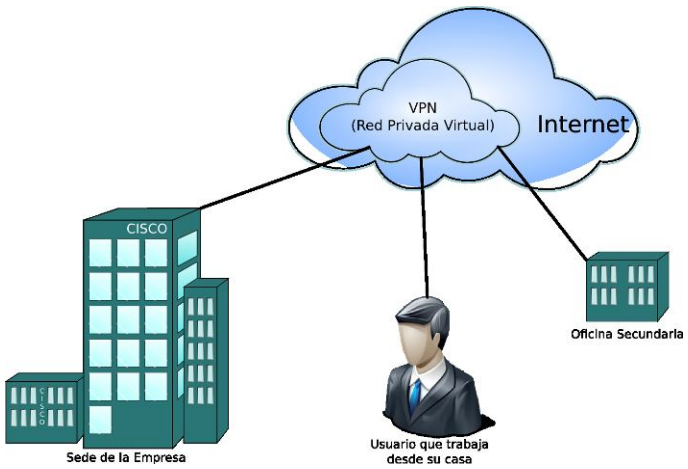

Figura 4.16: Red Privada Virtual

La VPN es un servicio que ofrece conectividad segura y confiable en una infraestructura de red pública compartida, como la Internet. Las VPN conservan las mismas políticas de seguridad y administración que una red privada. Son la forma más económica de establecer una conexión punto-a-punto entre usuarios remotos y la red de un cliente de la empresa.

A continuación se describen los tres principales tipos de VPN:

VPN de acceso: Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.

Redes internas VPN: Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados

de la empresa.

Redes externas VPN: Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

Capítulo 5

RADIUS

RADIUS Es un protocolo AAA (Autenticación, Autorización y Administración) para aplicacionescomo acceso a redes o movilidad IP.

Muchos ISP (proveedores de acceso a internet por dial up, DSL, cablemódem, ethernet, Wi-Fi, etc) requieren que se ingrese un nombre de usuario y contraseña para conectarse a la red. Antes de que el accesoa la red sea concedido, los datos de acceso son pasados por un dipositivo NAS (Network Access Server) sobre un protocolo de capa de enlace (como PPP, para muchos dialups y DSL), luego hacia un servidor RADIUS. Este chequea que esa informa- ción sea correcta usando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptada, el servidor autorizará el acceso al sistema del ISP y seleccionará una dirección IP, parámetros L2TP, etc.

RADIUS también es comúnmente usado por el NAS para notificar eventos como:

- El inicio de sesión del usuario.
- El final de sesión del usuario.
- El total de paquetes transferidos durante la sesión.
- El volumen de datos transferidos durante la sesión.
- La razón para la terminación de la sesión.

RADIUS es un protocolo de autentificación comúnmente utilizado por el estándar de seguridad del 802.1x (usado en redes inalámbricas). De todas maneras, RADIUS no fue creado inicialmente para ser un método de seguri-

dad en redes inalámbricas. RADIUS mejora el estándar de encriptación WEP, en conjunto con otros métodos de seguridad como EAP-PEAP.

5.1. Requerimientos

RADIUS utiliza UDP como su protocolo de base. El puerto registrado para tráfico de RADIUS es el 1812 (aunque inicialmente era el 1645 que entraba en conflicto con otro servicio). Cuando RADIUS ya autenticó al usuario, continúa "contabilizando" el uso de esa cuenta (Lo que en RADIUS se conoce como accounting), el puerto UDP registrado para esta etapa del servicio es el 1813 (aunque en un principio fue el 1646).

Este es un dato útil en el caso en el que el servidor RADIUS esté separado de sus clientes por un firewall, el administrador del firewall debe tener en cuenta que debe dejar pasar el tráfico hacia el radius a través de los puertos UDP 1812 y 1813.

5.2. Información Adicional

A los fines de este trabajo, solo usaremos RADIUS como una herramienta, explicar a fondo el funcionamiento de RADIUS pierde sentido ya que es demasiado extenso, de todas formas, si está a gusto del lector aprender de sus estándares de funcionamiento, recomendamos buscar:

- RFC 2865 Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868 RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 RADIUS Extensions
- RADIUS attributes and packet type codes (http://www.iana.org/assignments/radius-types)

Capítulo 6

DMZ

En seguridad informática, una zona desmilitarizada (DMZ, demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir, los equipos en la DMZ no pueden conectar con la red interna (LAN). Esto les permite dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la DMZ se convierte en un "callejón sin salida".

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando traslación de los puertos necesarios para evitar dejar totalmente expuestos los hosts que en ella se encuentran.

Una DMZ se crea a menudo a través de las opciones de configuración del firewall, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama firewall en trípode (three-legged firewall). Un planteamiento más seguro es usar dos firewall, donde la DMZ se sitúa en medio y se conecta a ambos firewall, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado firewall de subred monitoreada (screened-subnet firewall).

Resumiendo, por lo general, la política de seguridad de la DMZ es la siguiente:

El tráfico...

- ...Desde la red externa, por ejemplo internet...
  - ...Hacia la DMZ está **filtrado**
  - ...Hacia la LAN está **prohibido**
- ...Desde la LAN...
  - Hacia la DMZ está **autorizado**
  - Hacia internet está **autorizado**
- ...Desde la DMZ...
  - Hacia la LAN está **prohibido**
  - Hacia internet está **filtrado**

6.1. Entorno Doméstico

En el caso de un enrutador de uso doméstico[1], el "DMZ host" (O en algunas marcas DMZ Relay) se refiere a la dirección IP que tiene una computadora para la que un enrutador deja todos los puertos abiertos, excepto aquellos que estén explícitamente definidos en la sección NAT del enrutador. Es configurable en varios enrutadores y se puede habilitar y deshabilitar.

Con ello se persigue conseguir superar limitaciones para conectarse con según qué programas, aunque es un riesgo muy grande de seguridad que conviene tener solventado instalando un firewall por software en el ordenador que tiene dicha ip en modo DMZ.

Para evitar riesgos es mejor no habilitar esta opción y usar las tablas NAT del enrutador y abrir únicamente los puertos que son necesarios.

[1] Si bien este documento no está orientado a equipos domésticos, no se quiere evitar este comentario ya que es una duda que puede surgir al cruzarse con un equipo de menor categoría

Parte III

Desarrollo del Problema

Aquí mostraremos en detalle todas las configuraciones que se desarrollaron para lograr el producto final

Capítulo 7

Detalles de la red

Como ya se mencionó anteriormente, uno de los puntos importantes para tener en cuenta por parte del lector, es la evidencia que queda de la utilidad de trabajar con virtualización de equipos. En nuestra red (la cual por supuesto es un modelo a escala de la red propuesta) utilizamos como hardware un RouterBoard (Ver sección 8.3.1.2) y una laptop donde se virtualizarán algunos servidores y un RouterOS (Ver sección 8.3.1), esto puede verse diagramado en la figura 7.2.

Habiendo ya pasado por este documento, podemos definir los segmentos a utilizar, los productos, establecer la seguridad y bosquejar un esquema formal (ya conociendo los estándares de representación gráfica) de la red final. Se utilizan 2 redes para usuarios, una para personal de la empresa, otra para invitados (por supuesto con diferentes políticas de firewall). En el diseño se consideró además una red separada para servidores y una DMZ. La red puede crecer (de no agregarse subredes) hasta:

- 65534 Hosts de DMZ
- 65534 Servidores en LAN
- 65534 Clientes pertenecientes a la empresa
- 65534 Clientes invitados

De esta manera definimos lógicamente la red:

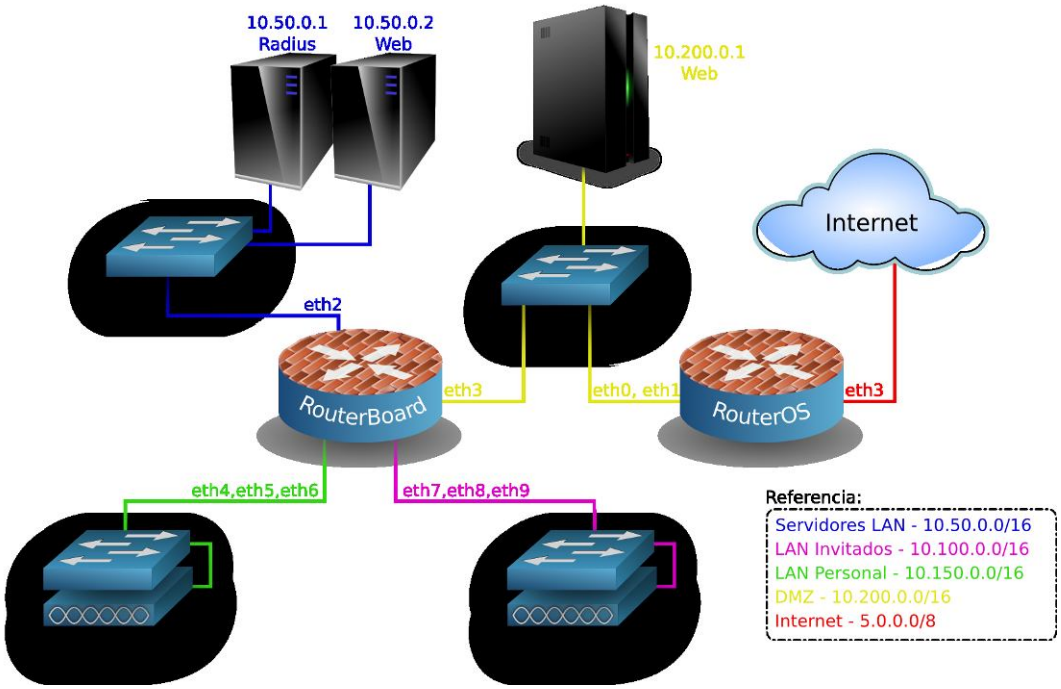

Figura 7.1: Esquema Lógico de la Red

Físicamente esto se traduce, como ya lo habiamos mencionado antes en este capítulo, en un RouterBoard y una laptop, dispuestos de la siguiente manera:

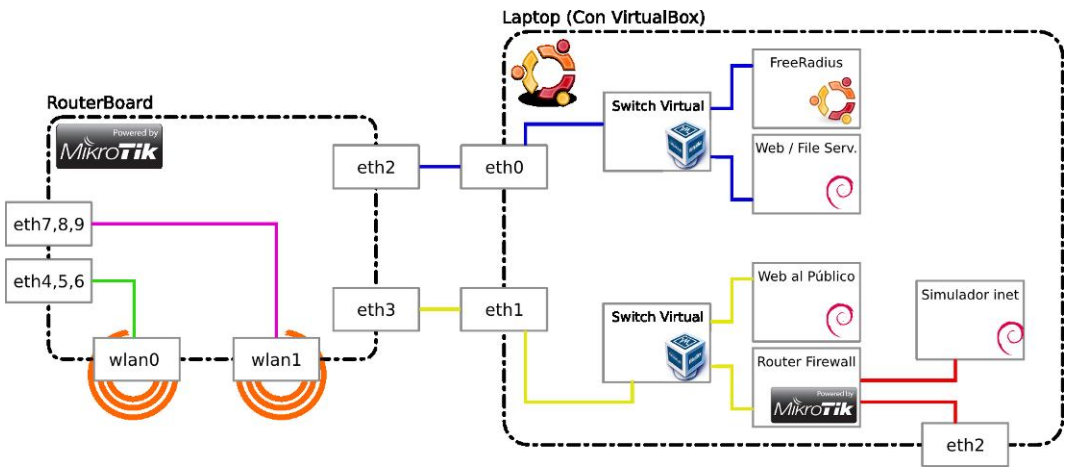

Figura 7.2: Esquema Físico de la Red

7.1. Planeamiento de las políticas del firewall

El firewall puede tomar, como modo global, dos políticas de filtrado diferentes:

Restrictivo: El firewall **NO PERMITE** pasar tráfico de ningún tipo excepto aquel que explícitamente se acepte.

Permisivo: El firewall **PERMITE** todo el tráfico excepto aquel que sea explícitamente denegado.

Por supuesto, por el ánimo de este proyecto, vamos a utilizar una política restrictiva, es decir, que debemos tomar nota de cuales son los servicios que queremos permitir para que éstos puedan ser explícitamente aceptados en el firewall. Por esto es conveniente hacer un buen análisis para la puesta en marcha.

7.1.1. Servicios en DMZ

En la DMZ dispusimos un servidor web, la idea es que éste brinde servicios hacia afuera de la red privada, es decir, que desde la eth2 de la laptop (Internet) puede accederse únicamente a ese equipo (10.200.0.1) en el puerto TCP 80 (http).

7.1.2. Servicios en LAN

Contamos con dos equipos, un servidor de archivos y web interna (10.50.0.2) y un servidor de RADIUS (10.50.0.1). El RADIUS debe poder accederse únicamente desde el RouterBoard ya que es éste el que le envia las consultas. Por otra parte, el servidor de archivos y web interna debe ser accedido unicamente por el personal (red 10.150.0.0/16). En conclusión, necesitamos aceptar TCP 80 (http) y TCP 445 (CIFS, Servicio de archivos compartidos de windows).

7.1.3. Servicios que brinda el Router

El RouterBoard además es capás de brindar algunos servicios de red a los clientes, en nuestro caso, cumple las funciones de DNS (Servicio de resolución de nombres), DHCP (Servicio de asignación dinámica de direcciones

de red) y PPTP (Servicio de Túnel punto a punto para VPN). Es decir que debemos considerar que en el firewall (ya veremos que el firewall tiene una sección de entrada, para protegerse a si mismo) permitir para las redes LAN de personal y de invitados los puertos UDP 53 (DNS), UDP 65-68 (DHCP), TCP 1723 y protocolo GRE (PPTP VPN).

Hay una cosa más, que muchas veces no se considera como servicio de red, sin embargo lo es, y es en este momento de diseño, lo más importante a tener en cuenta en las reglas de entrada al router, y es lo que usemos para administrarlo, si olvidamos aceptar Winbox, o SSH, o lo que sea que usemos para administrarlo, entonces ¡estaremos en problemas! Concluyamos de esto: NO OLVIDAR aceptar TCP 8291 (Winbox) y/o TCP 22 (SSH). Una nota importante es que estos puertos mencionados son los estándar, pero queda a la libertad del administrador del router cambiarlos a su preferencia, siempre y cuando no olvide modificar las reglas de firewall para no "perder el equipo", es decir, para que las reglas de firewall no impidan nuestra entrada al router: Por ejemplo, si tengo Winbox en el puerto 8291, con su regla "Aceptar TCP 8291" asociada, en caso de cambiar el servicio de Winbox del 8291 al 10000, debemos primero crear la regla "Aceptar TCP 10000" porque de otro modo no podremos entrar por ninguno de los dos puertos.

7.1.4. Reglas de estado

Recordemos que RouterOS posee un firewall de segunda generación, es decir, no solo entiende los paquetes individuales, sino que entiende con qué conexiones está relacionado ese paquete, o a que conexión pertenece, debido a esto, también entiende cuando una conexión es inválida (paquetes malformados y demás) que puede ser signo de que alguien está atacando la red. Por eso otra de las medidas a tomar en el firewall es aceptar las conexiones establecidas y relacionadas. Además, por más que las conexiones inválidas, por no estar aceptadas terminarán por descartarse, no está de más descartarlas explícitamente entre las primeras reglas para evitar que generen carga al microprocesador del router.

7.1.5. Reglas de LAN a DMZ y a Internet

La LAN es la red de mas alta seguridad, como ya dijimos el tráfico desde Internet o desde la DMZ está terminantemente prohibido hacia la LAN, sin embargo, desde la LAN es necesario que se puedan abrir conexiones hacia afuera para, por ejemplo, visitar una página web, leer correo, descargar actualizaciones, etc. Aquí entra mucho en juego el criterio del administrador, si bien la política podría ser aceptar todo lo que vaya hacia una zona de seguridad

menor, dijimos que seríamos restrictivos a la hora de poner en marcha los firewalls, es por esto que por nuestra parte decidimos aceptar lo que nos parece correcto para una organización (HTTP, IMAP, POP, SMTP, FTP) y para otras cosas estándar, dejamos las reglas "listas" pero deshabilitadas para que puedan ser habilitadas ante una necesidad y permitan el tráfico (P2P, MSN, Torrents).

7.1.6. Reglas para los Invitados

Esta vez entra de nuevo en juego el criterio del administrador y la definición de la compañía, en nuestro caso, y a modo de ejemplo (ya que una vez separada la red de invitados se puede filtrar o permitir lo que se desee) solo les permitiremos a los invitados navegar en internet, es decir NO a servidores de LAN.

7.1.7. Diseño Final

Recogiendo información de las secciones anteriores concluímos en que el firewall debe estar configurado de la siguiente manera:

En ambos routers, en todas direcciones:

- Denegar las conexiones inválidas
- Aceptar las conexiones establecidas
- Aceptar las conexiones relacionadas

Desde DMZ hacia LAN:

- Denegar Todo

Desde Internet hacia DMZ:

- Aceptar TCP 80 solo a la dirección de destino 10.200.0.1 (Web Pública)

Desde LAN hacia una zona de menor seguridad (DMZ o Internet):

- Aceptar TCP 80 y 443 (HTTP y HTTPS)

- Aceptar TCP 143 y 993 (IMAP e IMAPS)
- Aceptar TCP 110 y 995 (POP y POPS)
- Aceptar TCP 25, 465 y 587 (SMTP y SMTPS)
- Aceptar TCP 21 (FTP)

Desde LAN de Personal (10.150.0.0/16) hacia los servidores locales:

- Aceptar TCP 80 (HTTP)
- Aceptar TCP 445 (CIFS)

Hacia el RouterBoard:

- Aceptar UDP 53 (DNS)
- Aceptar UDP 65-68 (DHCP)
- Aceptar TCP 1723 (PPTP)
- Aceptar GRE (PPTP)

Capítulo 8

Puesta en Marcha

RESUMEN: Trataremos en este capítulo todo el detalle de configuración y selección de productos que se han realizado durante el desarrollo del problema

8.1. Debian GNU/Linux

Debian GNU/Linux es un sistema operativo libre, desarrollado por más de mil voluntarios alrededor del mundo, que colaboran a través de Internet. La dedicación de Debian al software libre, su base de voluntarios, su naturaleza no comercial y su modelo de desarrollo abierto la distingue de otras distribuciones del sistema operativo GNU. Todos estos aspectos y más se recogen en el llamado Contrato Social de Debian.

Nació en el año 1993, de la mano del proyecto Debian, con la idea de crear un sistema GNU usando Linux como núcleo ya que el proyecto Debian, organización responsable de su mantenimiento en la actualidad, también desarrolla sistemas GNU basados en otros núcleos (Debian GNU/Hurd, Debian GNU/NetBSD y Debian GNU/kFreeBSD).

Uno de sus principales objetivos es separar en sus versiones el software libre del software no libre. El modelo de desarrollo es independiente a empresas, creado por los propios usuarios, sin depender de ninguna manera de necesidades comerciales. Debian no vende directamente su software, lo pone a disposición de cualquiera en Internet, aunque sí permite a personas o empresas distribuir comercialmente este software mientras se respete su licencia. Debian GNU/Linux puede instalarse utilizando distintos mecanismos de instalación,

como DVD, CD, Blu-Ray, memorias USB y diskettes, e incluso directamente desde la red.

Actualmente muchas otras distribuciones de GNU/Linux son basadas en Debian, uno de los ejemplos mas significativos, quizás una de las distribuciones mundialmente mas difundida es Ubuntu. Ubuntu es un sistema diseñado para llegar al usuario final, lo que le da una cierta simplicidad de instalación y uso.

8.1.1. Ubuntu

Si bien Ubuntu no acostumbra usarse en servidores productivos, porque al ser un operativo destinado a ser sencillo posee mucho software adicional que puede resultar en una inestabilidad del sistema, hemos decidido utilizarlo, ya que, a los fines de este proyecto solo lo usamos como una herramienta, y no nos agregaría valor utilizar alguna otra distribución mas especializada para brindar servicios.

Pueden descargarse todas las versiones de Ubuntu desde http://www.ubuntu.com/download

8.2. FreeRadius

FreeRadius es un proyecto de software libre que contiene varios componentes, uno de ellos es el servicio de RADIUS. FreeRadius es el servicio de RADIUS más globalmente utilizado incluso por grandes compañías, y es por esto que existe muchísima documentación al respecto. Esta es una de las razones por las que lo elegimos para este problema.

8.2.1. Configuración de FreeRadius en Ubuntu Server

A continuación se listan los cambios realizados en los archivos de configuración de FreeRADIUS. El directorio de configuración es /etc/freeradius.

Las versiones de software utilizadas son las siguientes:

```
root@freeradius:~# lsb_release -a
Distributor ID: Ubuntu
Description: Ubuntu 10.04.1 LTS
Release: 10.04
Codename: lucid
root@freeradius:~# freeradius -v
freeradius: FreeRADIUS Version 2.1.8, for host
x86_64-pc-linux-gnu, built on Jan 5 2010 at 02:56:18
```

8.2.1.1. radiusd.conf

- **Configuración de proxy**: Esta función viene habilitada por defecto; se la deshabilitó usando la siguiente directiva:

```
proxy_requests = no
```

8.2.1.2. clients.conf

En este archivo el AP debe ser dado de alta para que el radius acepte sus consultas.

```
client 10.50.255.254 {
# tanto el AP como el radius tienen que tener
# el mismo secret.
secret = tecnicas3
shortname = AP
}
```

8.2.1.3. eap.conf

- Por defecto el tipo de autenticación EAP será PEAP.

```
default_eap_type = peap
```

- Copiar todos los atributos del paquete de autenticación original al túnel EAP.

```
copy_request_to_tunnel = yes
```

- Responder los atributos basado en el nombre de usuario dentro del túnel.

```
use_tunneled_reply = yes
```

- Las peticiones dentro del túnel se tratan por el mismo servidor virtual. comentar o eliminar la linea siguiente:

```
# virtual_server = ''inner-tunnel''
```

8.2.1.4. huntgroups

Permite diferenciar si el usuario es un empleado o un invitado.

```
personal NAS-IP-Address == 10.50.255.254,NAS-Port-Id == ''wls_personal''
invitados NAS-IP-Address == 10.50.255.254,NAS-Port-Id == ''wls_invitados''
```

8.2.1.5. users

Listado de usuarios (tanto empleados como invitados).

```
jorge Cleartext-Password := ''Password!'', Huntgroup-Name == ''personal''
gabriel Cleartext-Password := ''Password!'', Huntgroup-Name == ''personal''
felipe Cleartext-Password := ''Password!'', Huntgroup-Name == ''invitados''
```

8.2.1.6. servidor virtual sites-available/default

Se configuran las secciones authorize (determinar el tipo de autenticación, que será PEAP en este caso) y authenticate (validar el usuario). No se hace accounting.

```
authorize  preprocess #va a leer el archivo huntgroups pap #para hacer
pruebas desde una PC; no hace falta eap  #determina que Auth-Type = PEAP
ok = return
files #va a leer el archivo users
authenticate  #PAP: para hacer pruebas desde una PC; no hace falta
Auth-Type PAP
pap

#MS-CHAP: va a comprobar que la clave sea correcta
#dentro del tunel
Auth-Type MS-CHAP
mschap

#eap: PEAP es el tipo de autenticacion
eap
```

8.2.1.7. habilitar servidor virtual sites-available/default

Se habilita solamente el servidor virtual default.Para esto, dejar solamente un enlace simbólico a sites-available/default en sites-enabled.

8.3. Mikrotik

Mikrotikls Ltd., conocida internacionalmente como MikroTik, es una compañía letona vendedora de equipo informático y de redes. Vende principalmente productos de comunicación inalámbrica como routerboards o routers, también conocidos por el software que lo controla llamado RouterOS. La compañía fue fundada en el 1995, aprovechando el emergente mercado de la tecnología inalámbrica.

El principal producto de Mikrotik es el sistema operativo conocido como Mikrotik RouterOS basados en Linux. Permite a los usuarios convertir un ordenador personal PC en un router, lo que permite funciones comunmente utilizadas para el enrutamiento y la conexión de redes:

- Poderoso control QoS
- Filtrado de Trafico P2P
- Alta disponibilidad con VRRP
- Firewall Dinámico

- Túneles
- Red Inalámbrica de alta velocidad 802.11a/b/g con WEP/WPA
- Access Points virtuales
- HotSpot Para acceso Plug-and-Play
- Routeo RIP, OSPF, BGP, MPLS
- Configuración y Monitoreo en tiempo real

Existe un software llamado Winbox que ofrece una sofisticada interfaz gráfica para el sistema operativo RouterOS. El software también permite conexiones a través de FTP y Telnet, SSH y acceso shell. También hay una API que permite crear aplicaciones personalizadas para la gestión y supervisión.

8.3.1. Mikrotik RouterOS

8.3.1.1. Instalación del Sistema en una Máquina Virtual

Como ya se mencionó, RouterOS puede instalarse sobre una PC convirtiéndola en un router, ¿y por qué no utilizarlo sobre una máquina virtual? Utilizamos VirtualBox como plataforma de virtualizacion, VirtualBox es software libre, gratuito y multiplataforma que puede ser descargado directamente de la página web oficial: http://www.virtualbox.org/wiki/Downloads

Descargamos RouterOS desde la página web de Mikrotik:

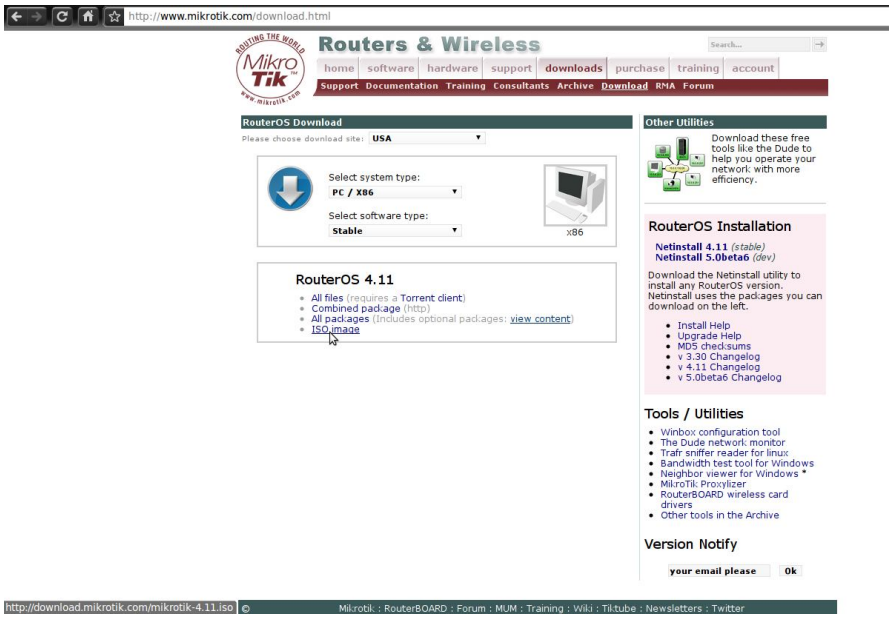

Figura 8.1: Descarga de RouterOS desde la página oficial

Creamos una máquina virtual nueva, RouterOS no requiere un disco muy grande, con 500MB es más que suficiente:

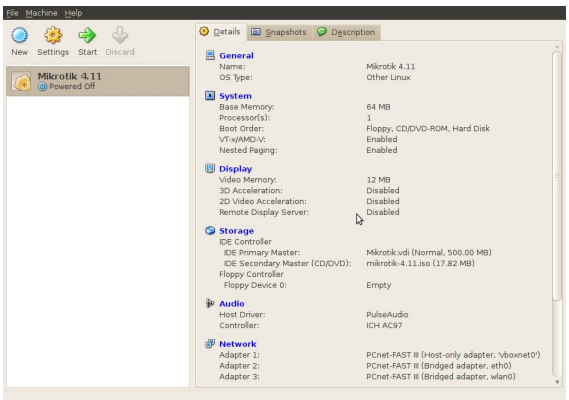

Figura 8.2: Administrador de Máquinas Virtuales de VirtualBox

Nos aseguramos de bootear la imagen iso descargada en la máquina virtual y la prendemos para instalar.

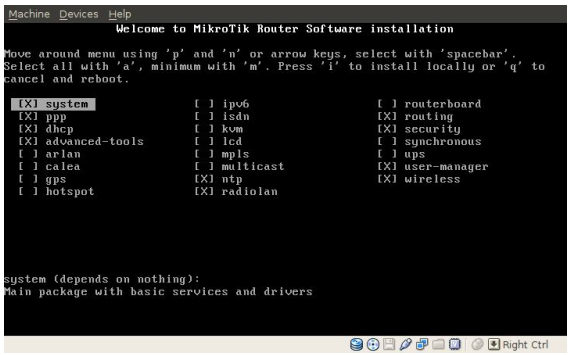

Figura 8.3: Selección de componentes de instalación

La instalación es sencilla, seleccionamos los paquetes a instalar, esperamos unos minutos, reiniciamos y listo, ya tenemos nuestro router corriendo, por supuesto falta la etapa de configuración que analizaremos mas adelante.

Tener en cuenta que las credenciales por defecto para RouterOS son admin sin contraseña.

La configuración de los Routers se detalla en las secciones 8.3.5 y 8.3.4.

8.3.1.2. Mikrotik RouterBoard

RouterBOARD es el nombre de una gama de productos de Mikrotik. Son placas base pensadas para construir routers. Suelen tener varios slots de expansión miniPCI para conectar tarjetas inalámbricas, puertos ethernet y USB. Algunos modelos más avanzados cuentan incluso con slots miniPCI-E para conectar tarjetas 3G. Por defecto, vienen con RouterOS preinstalado, pero se puede cambiar reprogramando la memoria flash interna a través del puerto serie.

Muchas comunidades inalámbricas optan por esta opción a la hora de crear nodos, pues son mucho más personalizables que los que se pueden comprar normalmente y se pueden ahorrar gastos en función de las necesidades que se tengan.

Además, suelen tener incorporada la tecnología Power over Ethernet (PoE) haciendo que sea posible, por ejemplo, alimentar el futuro router a través de un cable LAN RJ-45 estándar y eliminando así el uso de un alimentador de corriente convencional.

Usaremos como nuestro segundo router un RouterBOARD.

8.3.1.3. Medios de Configuración de RouterOS

Como ya se mencionó existen varias formas de administrar, configurar y monitorear un RouterOS:

Herramientas Gráficas

- Interfaz Web – Puerto 80
- Interfaz Web SSL – Puerto 443
- Winbox – Aplicación sobre puerto 8291
- API – Puerto 8728

Herramientas por Línea de Comandos

- SSH – Puerto 22
- Telnet – Puerto 23
- FTP – Puerto 21

Por seguridad, es recomendable dejar habilitado únicamente SSH y cambiar el puerto por defecto a otro cualquiera, pero para hacer una configuración inicial mas didáctica utilizaremos Winbox. Winbox es una aplicación de Mikrotik, gratuita, que corre bajo Windows:

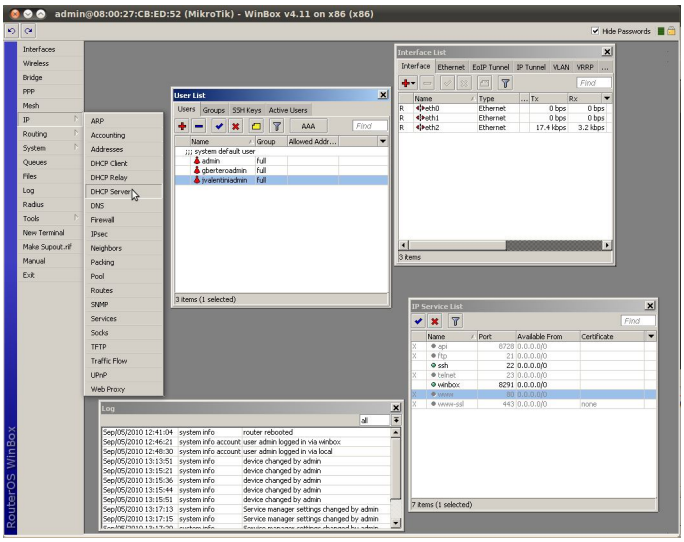

Figura 8.4: Winbox - Herramienta de administración gráfica de Mikrotik

8.3.2. Comenzando con MikroTik RouterOS

Aquí comienza el corazón de este problema, la configuración de RouterOS, aquellos que alguna vez hayan tenido la oportunidad de configurar un router hogareño saben que estos vienen preconfigurados para que sea muy sencillo hacer que funcionen (por supuesto sin las prestaciones ni la flexibilidad de un equipo industrial), por el contrario RouterOS no posee ningun tipo de pre-configuración, es por eso que puede ser complejo comenzar "de cero" con la configuración de RouterOS.

Una vez instalado el equipo (como se describió recientemente en la sección 8.3.1.1), nos encontraremos con un sistema virgen, cuyas credenciales por defecto son usuario admin y contraseña en blanco, y la dirección IP por defecto en la primer ethernet es 192.168.88.1. Para un usuario que recien comienza es recomendable utilizar Winbox para la configuración[1]. Instalamos Winbox, que puede descargarse gratuitamente de http://www.mikrotik.com/download/winbox.exe comenzamos...

[1]La administración por SSH es sencilla una vez que uno está habituado a la Winbox ya que la organización de las secciones son similares y la interfaz por línea de comandos es muy amigable

Figura 8.5: Pantalla de Login de Winbox

Por supuesto para poder llegar inicialmente al equipo debemos ponernos una ip del segmento 192.168.88.0/24 (que por supuesto no sea la 192.168.88.1), lo primero que debemos hacer es dar una contraseña al usuario admin (o mejor aún deshabilitar el usuario admin y crear usuarios nuevos con permisos de administrar), esto se controla desde **System / Users**:

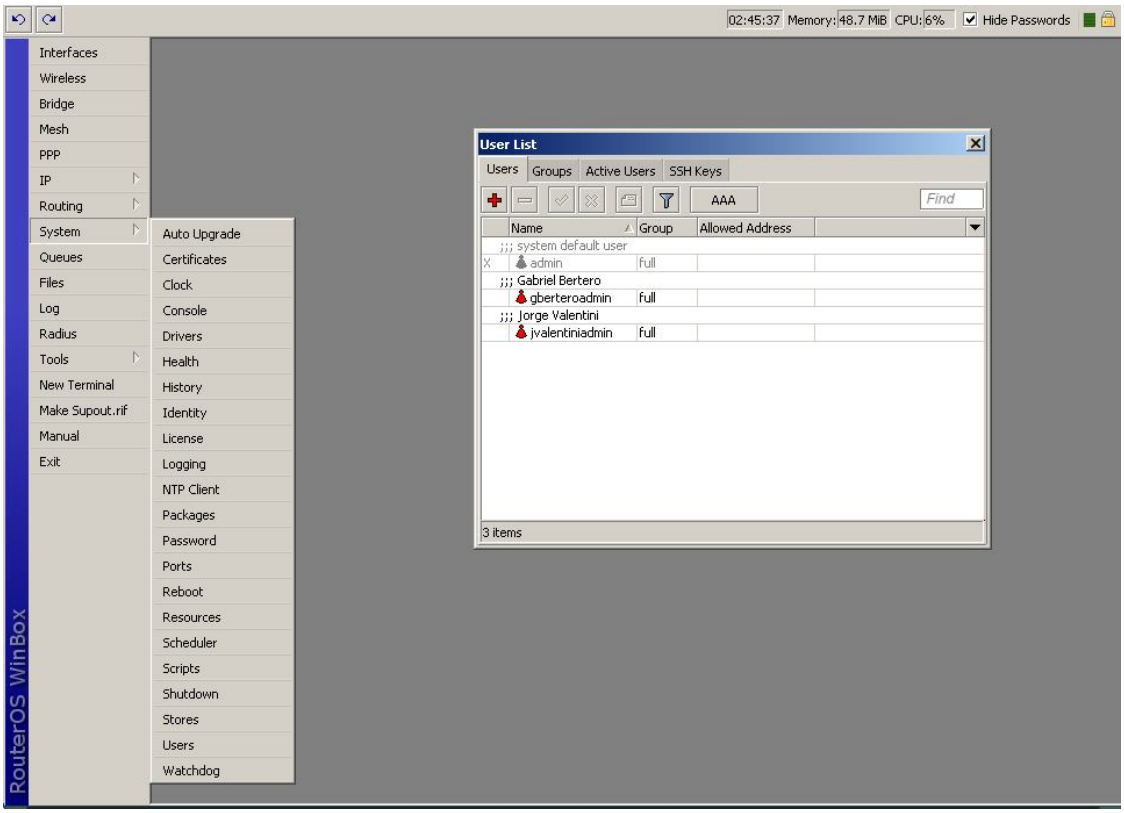

Figura 8.6: Gestión de Usuarios

Paso siguiente, Definir la función de cada una de las interfaces y comentarlas para evitar errores, esto se realiza desde la solapa **Interfaces**:

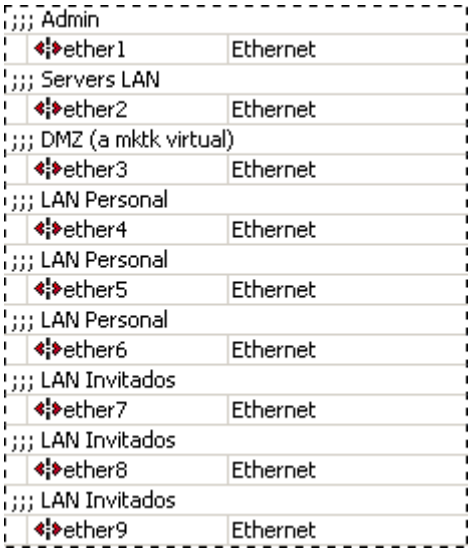

Figura 8.7: Interfaces de red

En los dispositivos con múltiples interfaces es recomendable crear "bridges", esto sirve para agrupar varias interfaces, de esta manera, si por ejemplo agrupamos las interfaces eth0, eth1 y eth2 en un bridge llamado "bridgetdiii", luego podremos asignar una ip o referir una regla de firewall sobre ese bridge y nos estamos refiriendo a las 3 interfaces, por eso, aunque en un primer momento asignemos una sola interfaz al bridge, esto tiene la ventaja de darnos flexibilidad para agregar interfaces a este bridge mas adelante. Los bridges se crean desde el menú Bridge, desde la solapa Bridge se crean los bridges y desde la solapa Ports se asignan las interfaces

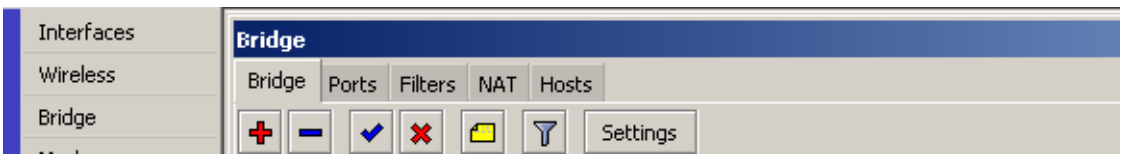

Figura 8.8: Agrupación de Interfaces

Una vez definidas las interfaces y los bridges iremos a definir la dirección o las direcciones IP del router, esta configuración se realiza desde el menú **IP / Addresses**. Cuidado, en este paso, si se cambia o deshabilita la ip 192.168.88.1 lógicamente se va a cortar la conexión y vamos a tener que reconectar el router a través de la nueva dirección. Para nuestros equipos definimos:

- RouterBoard Servers LAN - 10.50.255.254
- RouterBoard LAN Personal - 10.150.255.254
- RouterBoard LAN Invitados - 10.100.255.254
- RouterBoard DMZ - 10.200.255.254
- RouterOS Virtual DMZ - 10.200.255.253
- RouterOS Virtual Inernet - 5.5.5.5 (esta es solo una simulación)

Una configuración importante, es el horario, si el router tendrá acceso a internet, se recomienda configurar el cliente NTP (Protocolo de horario en red), que sirve para sincronizar la hora. Este puede ser privado o cualquiera de los tantos NTP públicos que existen (por ejemplo ntp.ubuntu.com ó time.afip.gov.ar). Esto se configura desde el menú **System / NTP Client**

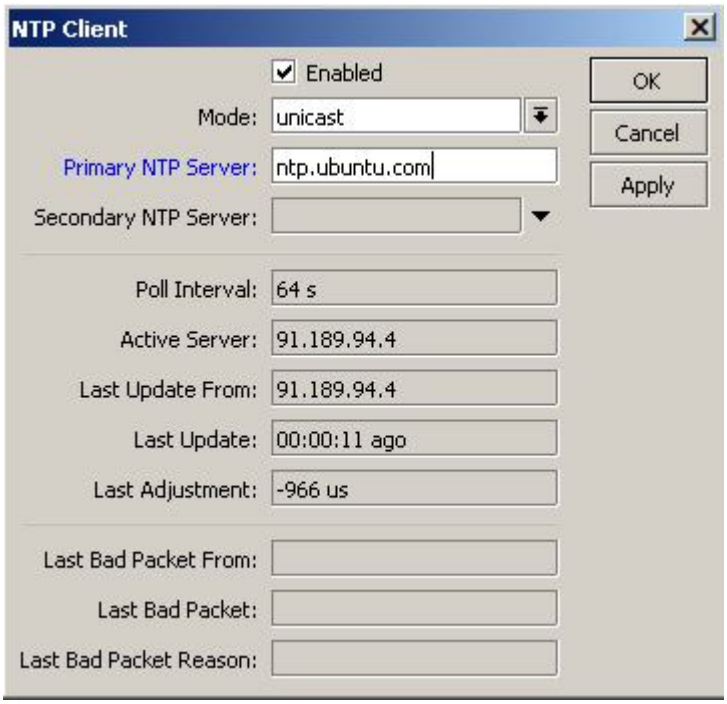

Figura 8.9: Configuración de Cliente NTP

A continuación, y como última medida de una puesta en marcha genérica, deshabilitemos los servicios innecesarios, como ya mencionamos, el equipo brinda servicios para facilitar su administración, muchos de ellos son inseguros y algunos simplemente innecesarios. Dejemos habilitados únicamente

Winbox y SSH, aunque si más adelante se puede dejar solo SSH, mejor aún. Este paso se hace desde el menú **IP / Services**:

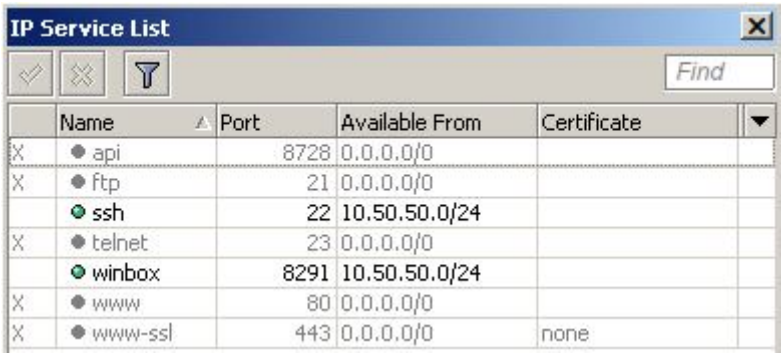

Figura 8.10: Servicios de RouterOS

Ya vimos las cuestiones que son generales a la configuración de un RouterOS, ahora vayamos en particular a los equipos que tenemos.

8.3.3. Configuración General del Firewall

Como ya dijimos, un firewall es aquel dispositivo que inspecciona el tráfico que recibe para evaluar si debe permitirlo o no, o dado el caso, hacer cualquier otra cosa como por ejemplo redirigirlo o saltar a otra evaluación o tan solo marcarlo con una cierta estampa. En mikrotik, el firewall se organiza en "tablas" (tables), "cadenas" (chains) y "reglas": La table clasifica la acción (hay 3 tablas disponibles y se muestran mas adelante), la chain es una clasificación global del tráfico, por ejemplo, "todo el tráfico que va dirigido hacia el Router" ó "Todo lo que viene de la LAN de invitados"; Las reglas son individualmente para cada tipo de paquete, que se permitirá y que no, por ejemplo, "Denegar cualquier paquete TCP que vaya dirigido al puerto 80 de cualquier equipo", nótese que hay una acción y una evaluación, la acción es denegar, y la evaluación es que el paquete cumpla con ser TCP 80.

Las tablas disponibles son:

TABLE	FUNCIÓN	CHAIN	DESCRIPCIÓN
Filter	Filtrado de paquetes	Input, Forward, Output	Filtra los paquetes dirigidos al firewall, que pueden accederse a través de otra interface del firewall, o que son originados por el firewall, respectivamente.
NAT	Traducción de direcciones	SrcNat, DstNat	Traduce la dirección de origen o destino, respectivamente
Mangle	Alteración de paquetes	Input, Forward, Output. Prerouting, Postrouting	Altera las cabeceras de los paquetes que entran, cruzan o se originan en el firewall, antes o después de enrutar el tráfico, respectivamente.

Tabla 8.1: Tables y Chains disponibles

Se debe especificar la table y la chain para cada regla de firewall creada, sin embargo las tablas están divididas, y siendo que las reglas habitualmente son de filtrado, la tabla de filtrado es aquella que aparece por defecto cuando vamos al firewall

Para ayudar a esta sección vea la figura 8.11 donde se considera un paquete que llega desde internet a nuestro firewall en una "red A" para comenzar una conexión.

Primero el paquete es evaluado por las reglas en la table mangle en la chain PREROUTING, en caso de que exista alguna. Luego se analiza por las reglas de la chain DstNat en la table NAT para evaluar si el tráfico requiere o no un destination NAT, es decir, una traducción de la red de destino. Luego de esto el paquete es enrutado.

Si el paquete está destinado a una red protegida, entonces este es filtrado por las reglas de filtrado de la chain FORWARD y, de ser necesario, el paquete pasa por la chain SrcNat de la table NAT antes de llegar a la "red B". Cuando el destino (en la "red B") decide responder a la petición iniciada se da la misma secuencia de pasos hacia atrás.

Si el destino del paquete inicial no es otra red sino el firewall mismo, entonces el paquete pasa por las reglas de mangle en la chain INPUT antes de pasar los las de filtrado. Si el tráfico llega exitosamente al firewall entonces este es procesado por el servicio en cuestión. En cierto punto, el firewall necesita responder a la petición, esta respuesta se enruta e inspecciona en las reglas de

la chain OUTPUT de mangle, luego por la DstNat y luego por la chain OUTPUT de la table filter. Finalmente, antes de mandar nuevamente el paquete a internet, pasa por la chain POSTROUTING de NAT y mangle.

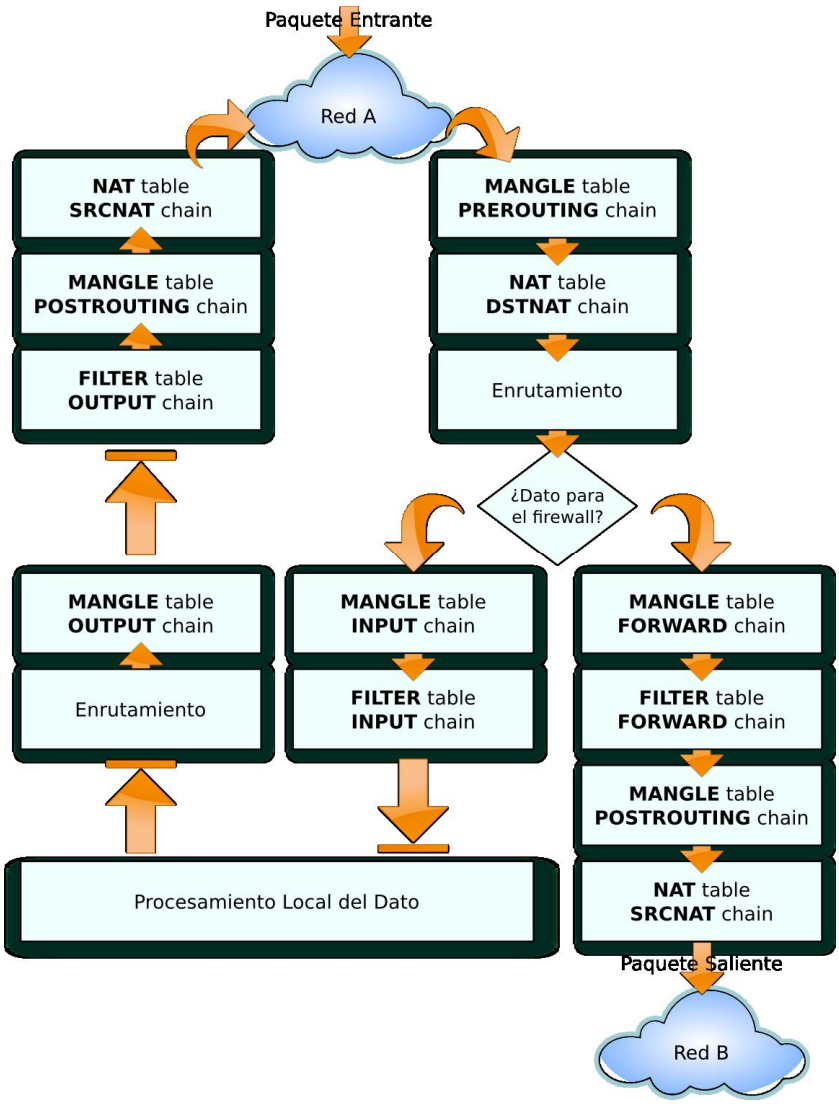

Figura 8.11: Flujo de los datos en el firewall

Como vimos anteriormente, las reglas de filtrado son las mas frecuentemente utilizadas, las chains que poseemos por defecto para trabajar son:

input Todo tráfico que va dirigido a cualquier interface del firewall

forward Todo tráfico que entra por una interface y sale por otra

output Todo tráfico que es iniciado por el router hacia afuera

Y las principales acciones (las mas utilizadas) que podemos tomar sobre un paquete son:

Accept Aceptar el tráfico

Drop Descartar el tráfico

Add Src to Address List Agregar la direccion de origen a una lista[2]

Add Dst to Address List Agregar la direccion de destino a una lista

Reject descartar el tráfico pero avisando al remitente del mismo

Jump Pasar a otra chain (que puede ser definida por el usuario)

Log Guardar un registro del tráfico

En la siguiente figura vemos la sección de configuración de filter rules, arriba a la derecha puede verse desplegado un menú para filtrar por chain:

Figura 8.12: Configuración de Reglas de Filtrado

Para la creación de Reglas tenemos las siguientes opciones, primero una solapa general (esto es fase de evaluación del tráfico) en la que podemos identificar dirección IP de origen o destino, protocolo (icmp, http, tcp, udp, gre, etc.), puerto, interfaces de entrada y salida, marcas en el paquete (ya veremos marcado de paquetes), tipo y estado de la conexión (recuerde que el firewall entiende estados, es de segunda generación):

[2] las listas de acceso (Access List) sirven como evaluación para el firewall, de este modo se puede decir, por ejemplo, "Aceptar Todo lo que venga de la Access List LAN" donde LAN contiene 10.50.0.0/16, 10.150.0.0/16 y 10.100.0.0/16

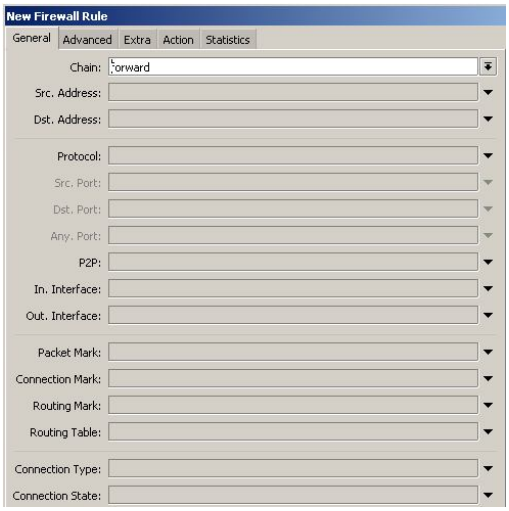

Figura 8.13: Nueva Regla - Configuración General

Luego tenemos la solapa "advanced" donde encontramos algunas cosas mas, como son muchas no vamos a describirlas todas, pero básicamente las mas utilizadas son lista de direcciones de origen y destino (ya veremos listas de direcciones o Address List), dirección MAC de origen, puerto de entrada o salida en un bridge, banderas TCP (esto sirve por ejemplo para saber si el paquete inicia, mantiene o cierra una conexión):

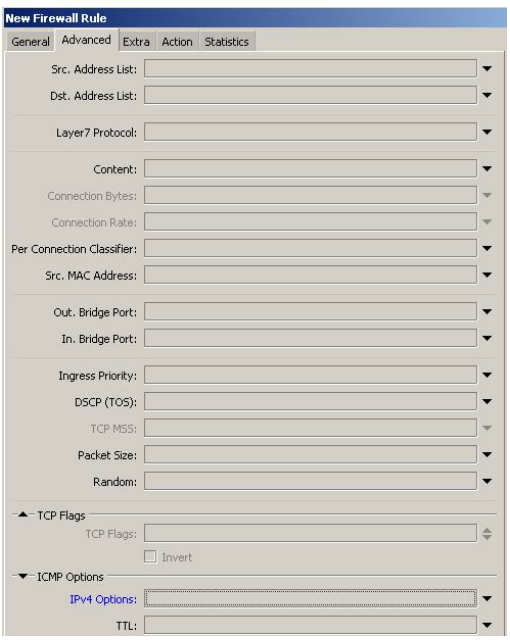

Figura 8.14: Nueva Regla - Configuración Avanzada

Por último entramos a la fase de acción del firewall, es decir, cuando el tráfico se evalúa y cumple con todas las condiciones que se establecieron en las anteriores configuraciones, entonces el firewall toma una decisión sobre ese paquete de datos, esto se establece desde la solapa action, donde se pueden utilizar cualquiera de las acciones descriptas item por item en la página 92

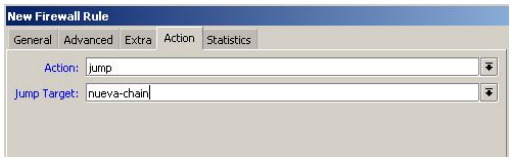

Figura 8.15: Nueva Regla - Acción

En orden de utilización le siguen las reglas de NAT, porque muchas veces es necesaria la traducción de una dirección. Por ejemplo, en nuestro caso, nosotros necesitamos que la direccion 10.200.0.1 pueda ser accedida desde internet en el puerto TCP 80, como bien sabemos una dirección IP de una red 10.200.0.0/16 es privada y por lo tanto no es accesible desde internet, lo único de nuestra red que se puede alcanzar desde internet es la pata pública del router que tiene la dirección 5.5.5.5. Para cumplir con el requerimiento lo que debemos hacer es una regla de NAT que traduzca la dirección publica a una privada, las traducciones se dividen en:

dstnat (destination NAT) Se traduce la dirección de destino.

srcnat (destination NAT) Se traduce la dirección de origen.

En el caso ejemplificado, lo que se necesita es un destination NAT, es decir, en un paquete que posee una dirección de origen y una dirección de destino debemos traducir o modificar la dirección de destino (de la 5.5.5.5 a la 10.200.0.1), entonces nuestra regla será: “Todo tráfico que venga desde internet, y que esté dirigido a la dirección 5.5.5.5 en el puerto TCP 80, modificar su dirección de destino por la 10.200.0.1 en el puerto 80”. Expresarlo con palabras es mas difícil que implementarlo:

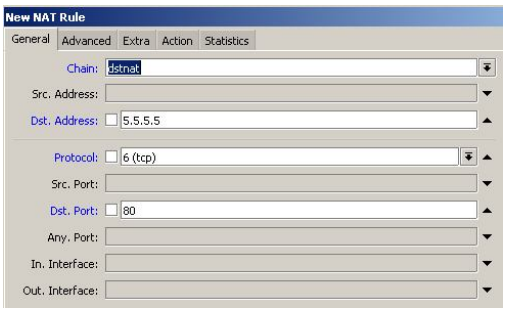

Figura 8.16: Regla de NAT - Evaluación

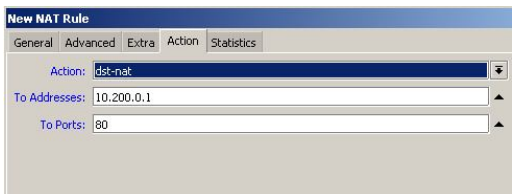

Figura 8.17: Regla de NAT - Acción

Por último tenemos la tabla de marcado (mangle) que tiene por principal fin marcar paquetes para futuras acciones sobre el. Si bien para lo que mas se usa es para priorización de tráfico (QoS), también puede usarse para el firewall a los fines de mantener todo organizado, por ejemplo, una regla que dice "Denegar todo el tráfico al puerto TCP 80" puede reemplazarse por "Marcar como –DENEGAR– el tráfico al puerto TCP 80" y luego "Denegar todo tráfico marcado como –DENEGAR–", de esta manera se puede llegar a obtener un conjunto de reglas mas ordenadas. El Mangle es raramente utilizado en entornos pequeños.

8.3.4. Configuración del Router a la LAN

Configuramos los Bridges y comentamos las interfaces, luego configuramos las IP como se vio anteriormente:

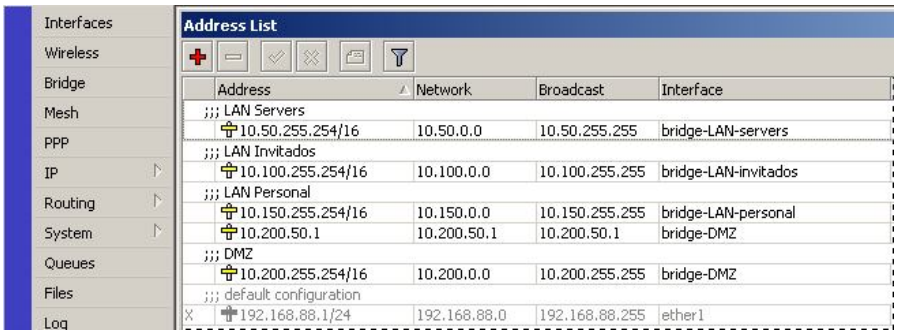

Figura 8.18: Direcciones del equipo

8.3.4.1. DNS

Ponemos en marcha el servicio de DNS, como ya se comento anteriormente, DNS es un servicio de traducción de nombres (que pueden recordarse fácilmente por humanos) a direcciones IP. DNS es un servicio complejo de capa 7 en el que no vale la pena ahondar ya que generalmente en las redes de control (aquellas utilizadas por electrónicos) no se utiliza para evitar un punto de falla y se utilizan direcciones IP directamente. Sin embargo, como en muchos ambientes es mandatoria la utilización de DNS (Por ejemplo Internet), no podemos pasarlo por alto en este documento.

Miktrotik Router OS no es el producto mas indicado para dar servicios de DNS, sin embargo posee la capacidad de darnos algo sencillo de poner en marcha, y no por eso menos efectivo:

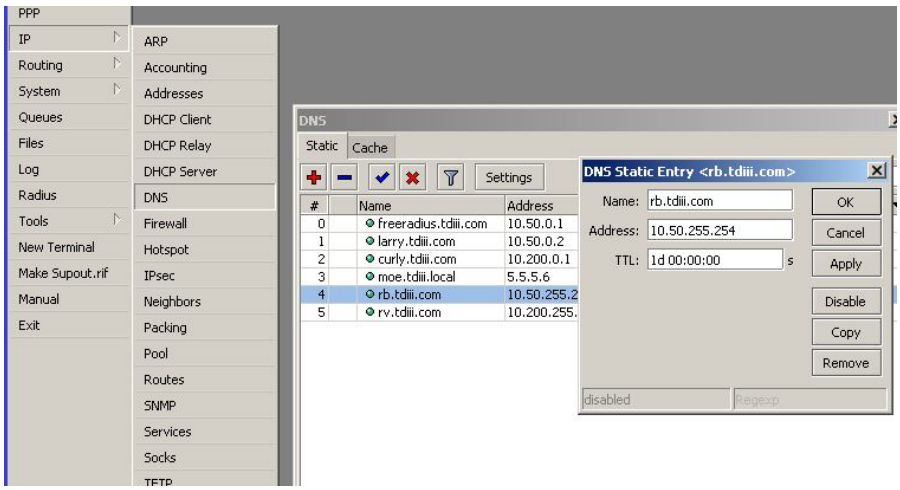

Figura 8.19: Serivico de DNS

Como se muestra en la figura anterior, configurar el DNS es sencillo, uno lo habilita, luego crea entradas estáticas donde especifica el nombre con el que se reconocerá a un equipo en la red y su dirección IP.

8.3.4.2. DHCP

DHCP es un servicio que permite asignar dinámicamente las direcciones IP a una red, es, como DNS, un servicio prácticamente indispensable en una red grande. El DHCP toma un rango de direcciones dentro de una red, y mantiene una base de direcciones IP relacionadas con direcciones de capa 2 (MAC), de esta manera conoce que direcciones están tomadas y cuales están disponibles.

DHCP significa "Protocolo de configuración dinámica de equipos" y, su nombre indica que debe hacer algo mas que solo configurar IPs, en efecto lo hace, puede configurar muchos parámetros de una placa de red de un equipo, por ejemplo, su puerta de enlace, sus servidores de DNS, WINS, servidores PXE para booteos desde la red, entre muchísimas otras opciones mas.

Para configurarlo debemos comenzar por definir la red en la que tomará su rol el DHCP (En nuestro caso la red de invitados y la red de personal), esto lo hacemos desde el menu **IP / DHCP Server** en la solapa Networks:

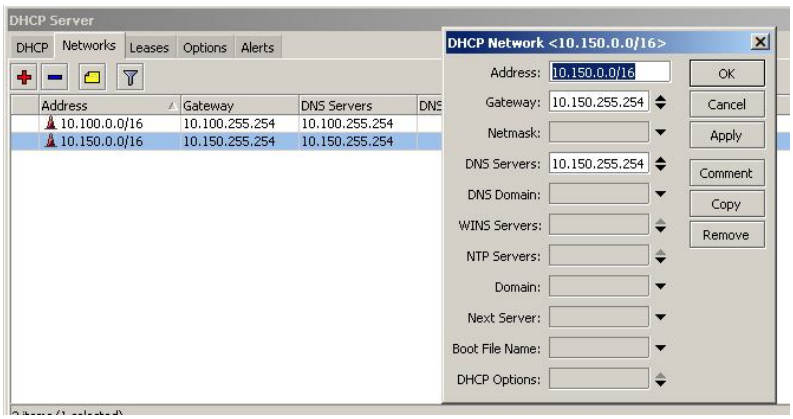

Figura 8.20: Redes del DHCP

El segundo paso es definir el rango para la red, es decir, cuales son las direcciones que el DHCP está habilitado para brindar. Esto puede o no ser la red completa. Muchas veces pueden utilizarse 2 o mas servidores de DHCP en la red y estos no deben superponer sus rangos, ya que cada uno de ellos tiene documentadas las direcciones que entregó, pero no las que entregó el

otro, por ejemplo, en la red 192.168.0.1/24, podría tener un DHCP que entregue direcciones entre la 192.168.0.1 y la 192.168.0.19, si deseara poner otro DHCP en la misma red, deberia usar un rango que vaya como máximo de la 192.168.0.20 a la 192.168.0.254. Esto es totalmente hipotético ya que suelen dejarse direcciones fuera del rango de cualquiera de los DHCPs, para, por ejemplo, el mismo servidor de DHCP.

Configuramos entonces los rangos de IP que entregarán nuestros DHCPs, que como ya mencionamos son dos, el de la red de invitados y el de la red de personal, esto se hace desde el menú **IP / Pool**:

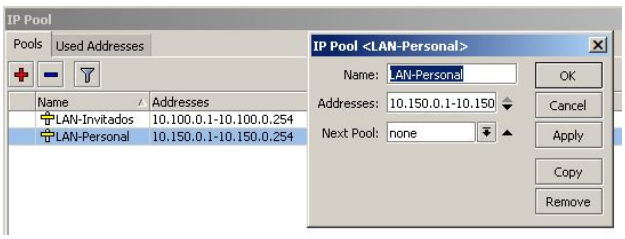

Figura 8.21: Rango de alquiler del DHCP

como último paso en la configuración del DHCP, es definir el servicio propiamente dicho, en él, se asinga un rango de los previamente establecidos, esto se agrega desde el menú **IP / DHCP Server** en la solapa DHCP :

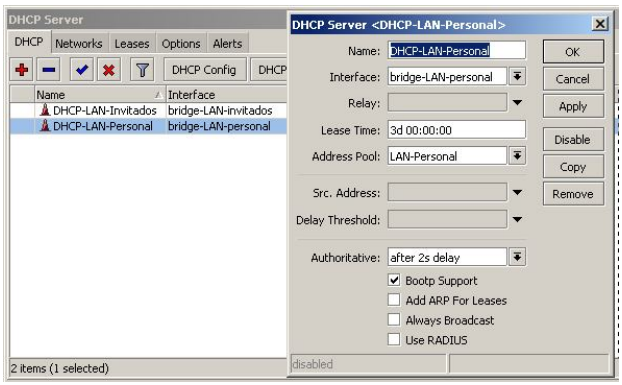

Figura 8.22: Servicio de DHCP

8.3.4.3. PPTP

PPTP es un protocolo de túnel que se utiliza en redes privadas virtuales (VPN, vea la sección 4.6). Mikrotik permite validar usuarios para habilitar

un túnel PPTP, el cual, cabe reiterar, es una vía segura de comunicación entre una red pública y una privada (o bien dos privadas a través de una pública). Los pasos para configurarla en el Router son:

Primero que nada, habilitar las consultas remotas en caso de que el equipo brinde servicios de DNS, esto significa que debemos controlar las consultas desde redes indeseadas mediante el firewall. Esto se hace desde el menú **IP / DNS** en el botón Settings:

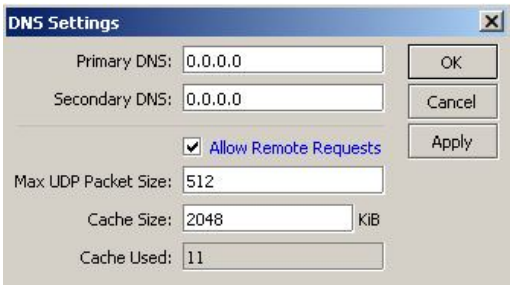

Figura 8.23: DNS - Aceptar peticiones remotas

Seguimos por el firewall, es necesario habilitar el puerto de servicio para PPTP (desde la solapa Service Ports):[3]:

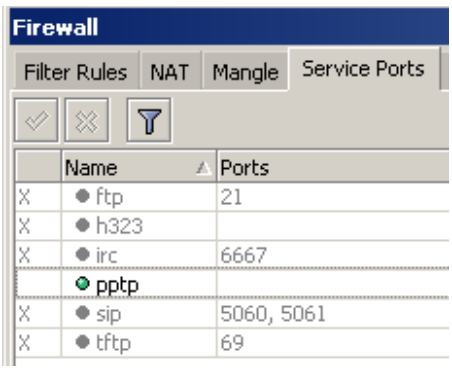

Figura 8.24: Firewall - Puertos de Servicio

Ultimo paso de preparación para comenzar con PPTP: Crear un pool de direcciones IP para los clientes PPTP, al igual que como se realizó para DHCP, esto se hace desde el menú **IP / Pool**:

[3] en caso de tener reglas de filtrado en la chain de input agregar la excepción para protocolo GRE y Puerto TCP 1723 (conexiones requeridas por pptp). Véase el apartado 8.3.4.4

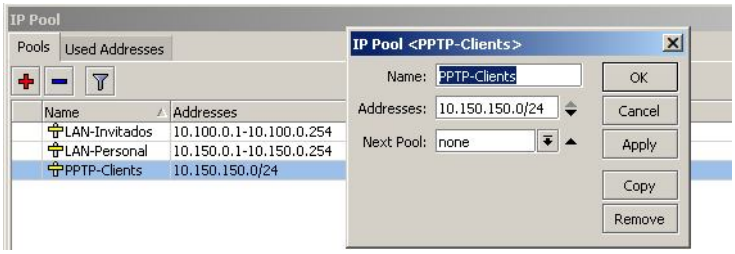

Figura 8.25: IP Pool - Direcciones para clientes PPTP

En las configuraciones de PPTP podemos notar 3 divisiones: el perfil de la conexión (IPs, DNS, encriptación, etc), la interfaz virtual del servicio y los usuarios para validar[4].

Primero se crea el perfil:

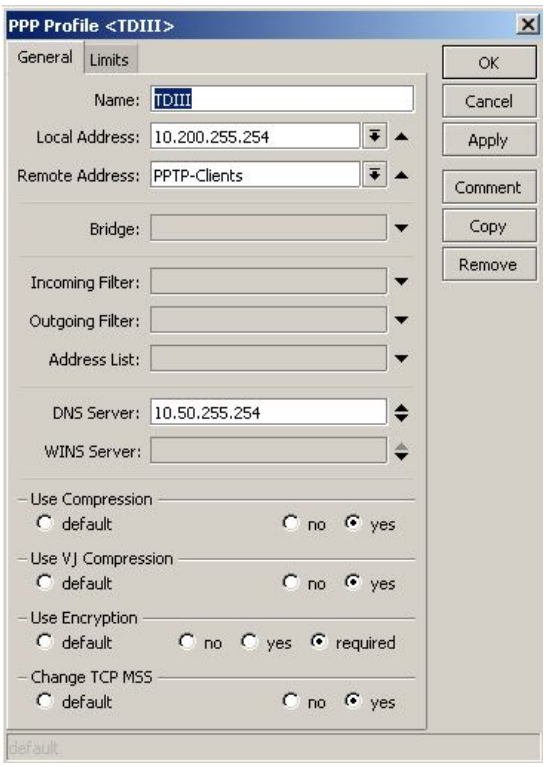

Figura 8.26: PPTP - Perfil de conexión

[4]PPTP también puede validar con RADIUS, pero a los fines de este problema nos pareció mas visual configurarlo con usuarios locales en el Mikrotik

A continuación, creamos la interfaz del servicio, desde la solapa Interface, primero configuramos el PPTP desde el botón PPTP Server y luego agregamos la interfaz, este último paso no requiere ningun tipo de configuración mas el que el nombre, entonces:

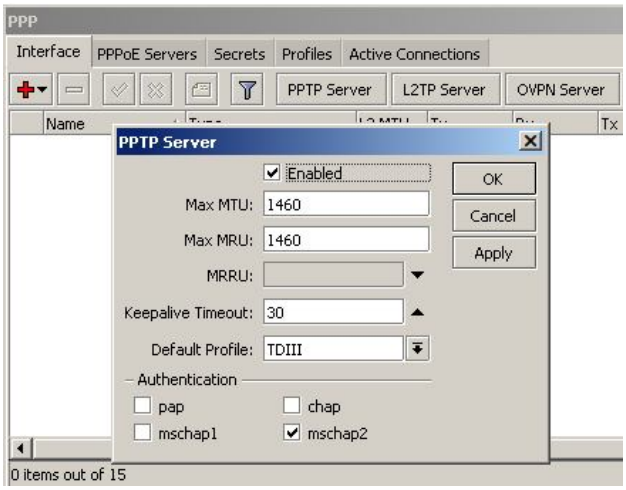

Figura 8.27: PPTP - Configuración del servicio

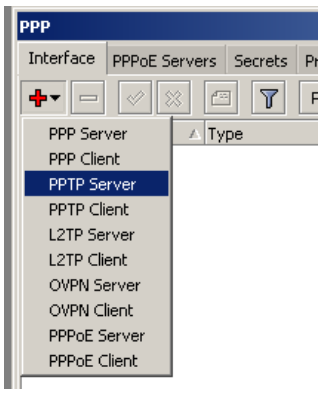

Figura 8.28: PPTP - Agregar Interfaz

La infraestructura para el túnel ya está lista, lo único que falta es crear los usuarios, esto se hace desde la solapa Secrets

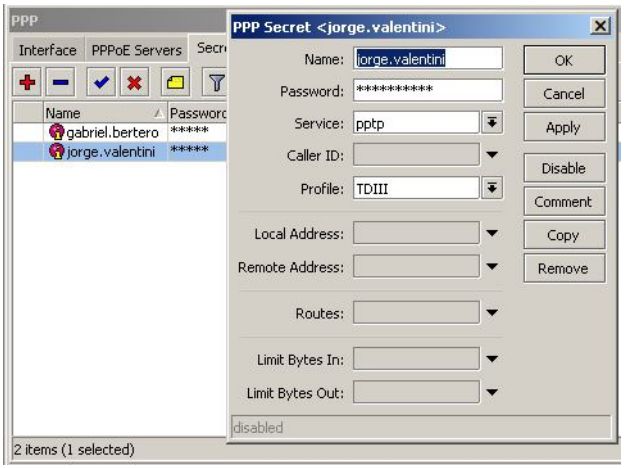

Figura 8.29: PPTP - Agregar Usuarios

8.3.4.4. Firewall

Como el Firewall es una de las cuestiones mas importantes en lo que hacen a este dispositivo de red, es por esto que su configuración general se describió en la sección anterior y aquí solo nos limitaremos a ingresar las reglas que pensamos en el diseño de la sección 7.1.7. Entonces, ingresaremos las reglas organizadas de la siguiente manera:

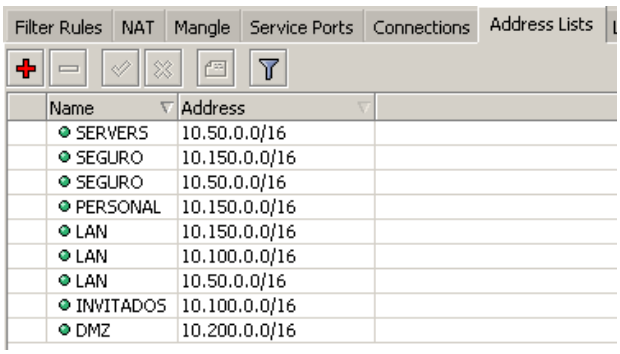

Figura 8.30: Listas de Direcciones

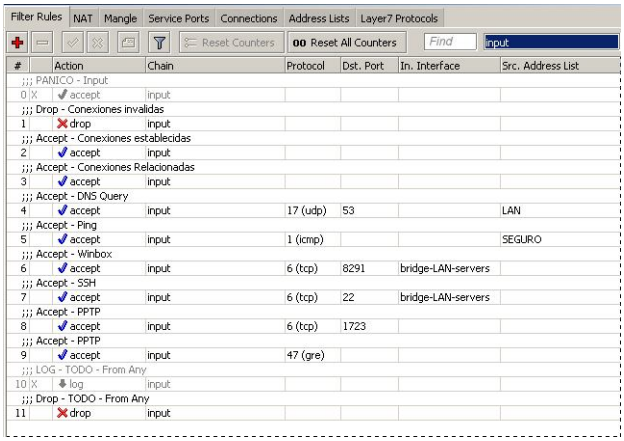

Figura 8.31: Reglas de Input

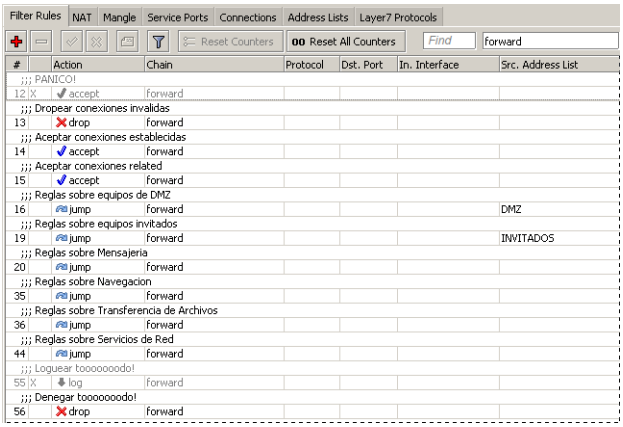

Figura 8.32: Reglas de Forward

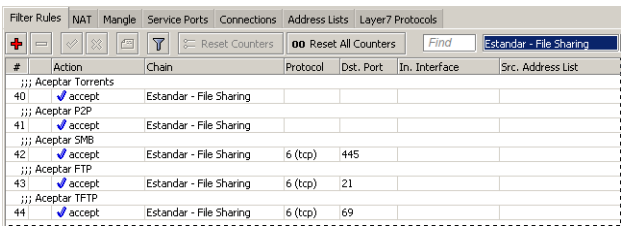

Figura 8.33: Reglas de Transferencia de archivos

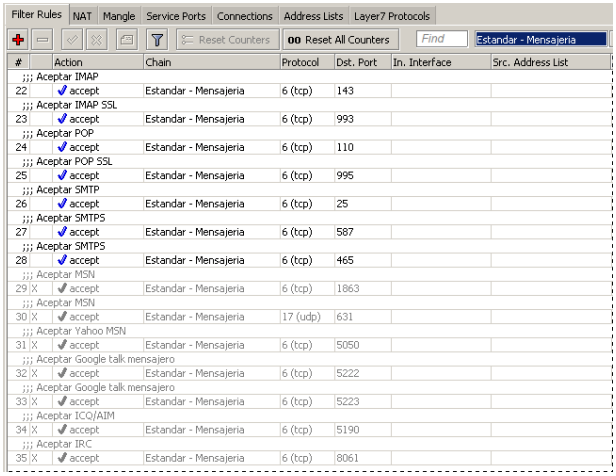

Figura 8.34: Reglas de Mensajería

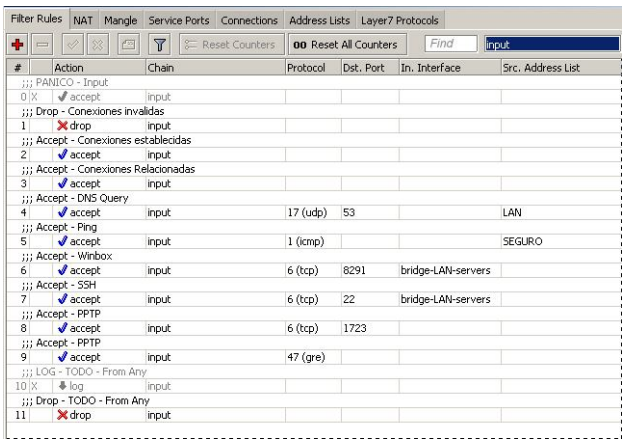

Figura 8.35: Reglas de Servicios de Red

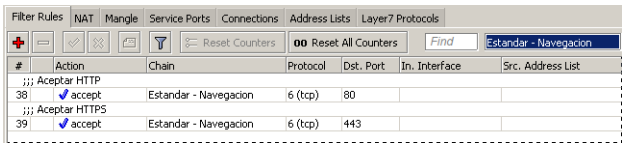

Figura 8.36: Reglas de Navegación

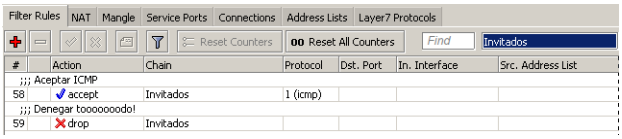

Figura 8.37: Reglas de Invitados

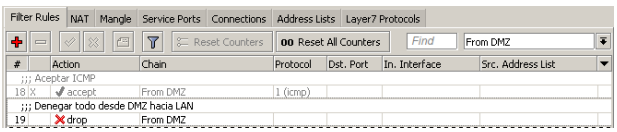

Figura 8.38: Reglas de DMZ

Nótese la utilización de listas de direcciones y reglas de salto para mantener todo organizado, además nótese que se dejaron algunas reglas deshabilitadas, estan dispuestas a los fines de dejarlas como documento, para que si en algun momento desea dejar de filtrarse por ejemplo, el servicio de messenger (msn) pueda habilitarse sin necesidad de loguear o investigar el servicio, simpemente habilitando la regla.

8.3.5. Configuración del Router a Internet

El router que se encuentra entre la DMZ e internet, no posee grandes configuraciónes, ya que su principal función es la de firewall, y como ya hemos mostrado suficientes datos sobre firewall creemos que pegar las reglas (que son muy similares) no agrega valor al documento. Lo que si agrega valor es mostrar lo que este otro equipo incluye de nuevo, y es el NAT.

Recordemos que este equipo traduce las direcciones de internet para los clientes y de la DMZ para los clientes que provienen de internet así que es en este equipo que vemos el NAT en acción. Un equipo que está en internet, para acceder a la web de la DMZ, no puede apuntar al equipo 10.200.0.1, porque de ninguna manera conoce esa red que es privada, lo que debe hacer es dirigirse a la ip 5.5.5.5 (IP del firewall en internet) y este debe saber, que una consulta que le llegue, a determinado puerto, debe pasarla al equipo 10.200.0.1, es decir, debe traducir la dirección de destino (dstnat):

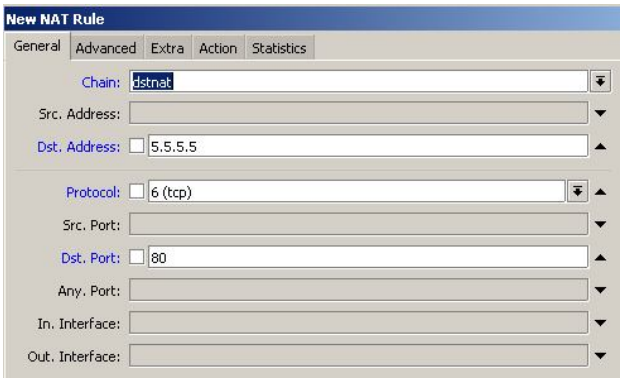

Figura 8.39: Destination NAT

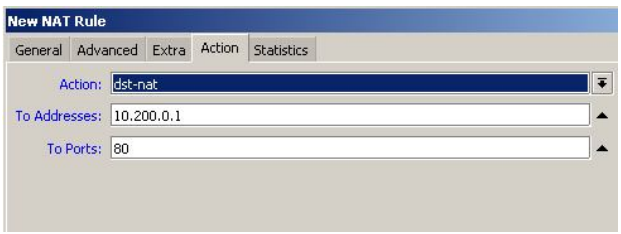

Figura 8.40: Destination NAT

El mismo caso es para PPTP, el servicio para la VPN lo da el RouterBoard (LAN-DMZ), debemos hacer un destination nat para TCP 1723 y GRE

Además, debemos enmascarar los clientes con la ip pública para que sean capaces de navegar, si un paquete de la 10.150.0.1 hace una petición de http a google.com directamente, sin ser enmascarado, google.com puede intentar devolver esa petición (si es que no la filtra) pero nunca va a saber como llegar a la dirección 10.150.0.1 porque es privada. Lo que se utiliza es la traducción de la dirección de origen, haciendo que todo lo que venga de la 10.150.0.0/16 se enmascare con la IP pública del mikrotik: la 5.5.5.5. Para decirlo de otro modo, en internet, toda maquina de nuestra red, se identificará con la IP 5.5.5.5, y es el firewall que está en esa dirección el que se encarga de entregarlo al destinatario original. Entonces la regla es toda ip de origen que sea de una red privada, en la chain srcnat, será enmascarada (action=masquerade).

En este punto vamos a permitirnos volver atrás, llamando a la reflexión, según todos los conceptos que se han visto en este documento, ¿Es correcto que la DMZ, por más que esté filtrada, conozca las rutas hacia las redes internas de mayor seguridad? La respuesta es "no", si lo pensamos bien, cuando un equipo desde una red segura abre una conexión hacia la DMZ, la respuesta

del equipo de DMZ caerá en la regla de "Aceptar Conexiones Establecidas", y por lo tanto estaremos violando la regla más mandatoria de una DMZ: No se permiten conexiones a las redes mas seguras. Es por esto que, si bien no se agregó en la sección anterior, donde se trata la configuración del RouterBoard, no estará de más si volvemos para hacerle un Source Nat que enmascare todo el tráfico con la IP de DMZ del Router (10.200.255.254).

8.4. Configuración de los Clientes

8.4.1. Wi-Fi

Recordemos que la Wi-Fi se configuró como WPA2 Enterprise con encriptación AES, validando usuario y contraseña sin certificado, tanto para la red de personal como para la red de invitados. Esto se configura en el cliente de la siguiente manera[5]:

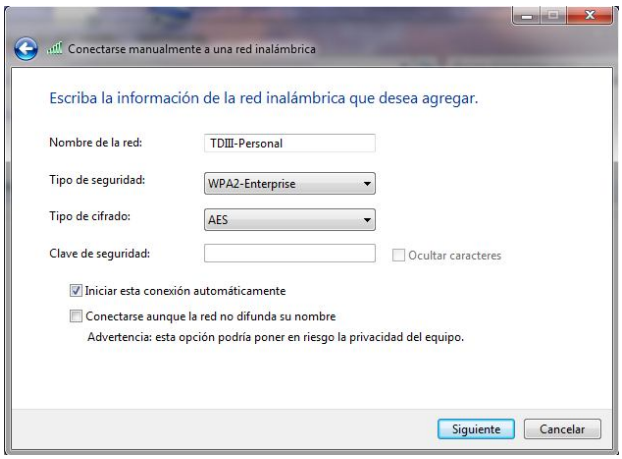

Figura 8.41: Configuración de Clientes - WiFi

[5]Las capturas de pantalla son tomadas bajo Microsoft Windows 7 Professional, en la versión Windows XP Service Pack 3 ya se puede conectar a redes WPA2 Enterprise y la configuración es muy similar

Figura 8.42: Configuración de Clientes - WiFi

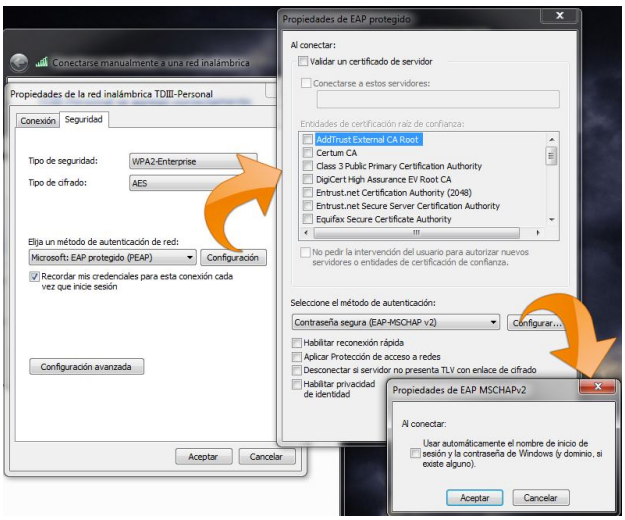

Figura 8.43: Configuración de Clientes - WiFi

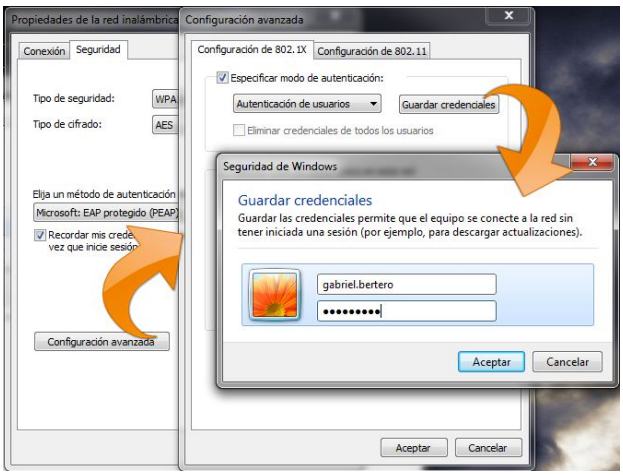

Figura 8.44: Configuración de Clientes - WiFi

8.4.2. VPN

Recordemos que la conexión VPN es PPTP con cifrado y validación mediante MS-CHAPv2. Para configurarla en el cliente, vamos a "Conexiones de Red", "Crear una Conexión Nueva".

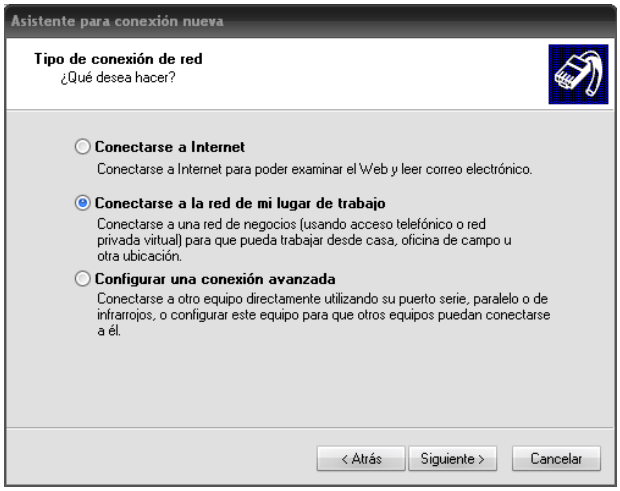

Figura 8.45: Configuración de Clientes - VPN

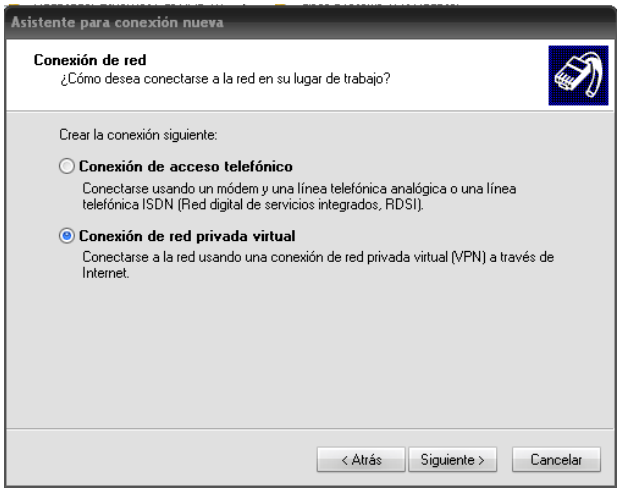

Figura 8.46: Configuración de Clientes - VPN

Luego nos solicita:

Nombre de la Organización: Es solo un nombre para reconocer la conexión,

nosotros elegimos TDIII.

Red Pública: Se refiere a la conexión que utiliza antes de conectar a la VPN, tildar "No usar la conexión inicial".

Nombre de Host o IP: Es el servidor de pptp, ingresar vpn.tdiii.com ó 5.5.5.5.

Eso crea una conexión con valores por defecto, para reforzar la seguridad:

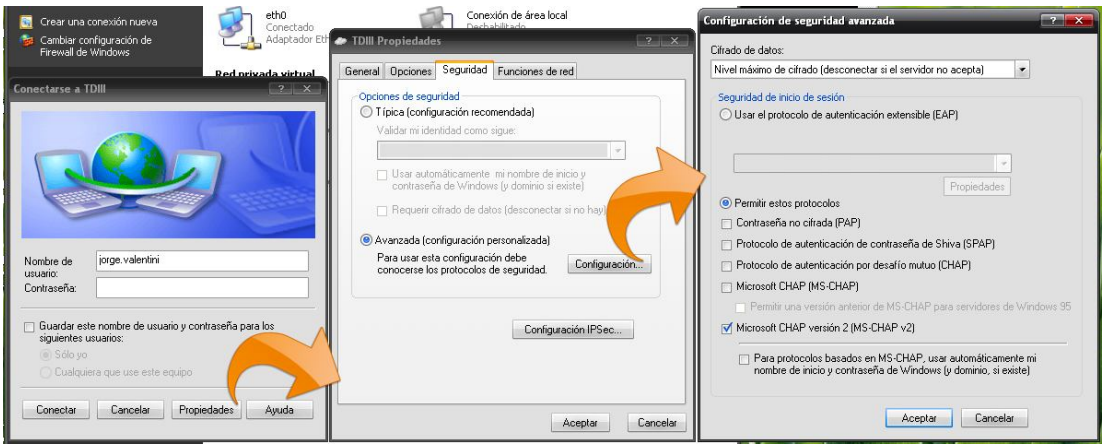

Figura 8.47: Configuración de Clientes - VPN

Ingresamos nombre de usuario y contraseña y listo, un icono celeste nos muestra que la conexión ha sido exitosa.

Figura 8.48: Configuración de Clientes - VPN

Capítulo 9

Pruebas y Medidas de Seguridad

RESUMEN: Administrar la seguridad de una red es un problema muy extenso que siempre queda en las manos del personal más especializado, tal es así que no podemos pretender mostrar demasiado sobre este tema, sin embargo, haremos lo posible por mostrar en este capítulo, las formas mas básicas de controlar la seguridad de la red.

El primer paso para mejorar la seguridad de una red es conocer sus vulnerabilidades, para poder recién en ese momento, y si está a nuestro alcance, mitigarlas. Para esta tarea, se procedió de la siguiente manera:

9.1. Evaluación de los Servicios

Corroboramos mediante la utilización de los servicios que no quede nada abierto de manera grosera hacia redes que no corresponda. Para esto, fuimos "poniéndonos" en las distintas redes y probando los servicios[1].

[1] Cuando uno piensa en seguridad de una red, instantáneamente piensa en intrusos o en ataques, pero la seguridad también engloba que los servicios permitidos se mantengan disponibles, es decir, debemos asegurarnos que nadie sin derechos pueda acceder y que nadie con derechos se vea imposibilitado de usar los servicios.

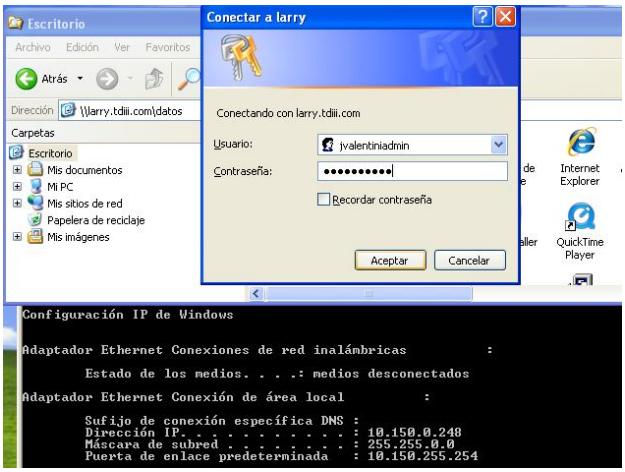

Figura 9.1: Acceso a Archivos Compartidos

Figura 9.2: Acceso a Archivos Compartidos

Nótese como, desde la red de personal (10.150.0.0/16) puede accederse al servidor de archivos compartidos (larry.tdiii.com, en la ip 10.50.0.2, que da los servicios de archivos e intranet). Sin embargo, veamos en la siguiente figura, que conectándose a la red de invitados (si bien el equipo se puede alcanzar, lo que queda evidenciado en los ping de la izquierda) es imposible acceder al mismo:

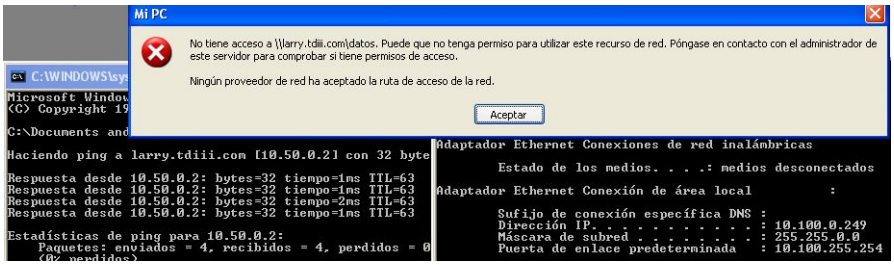

Figura 9.3: Acceso a Archivos Compartidos

De la misma manera probamos con la intranet, de la misma manera, se la puede acceder desde la red de personal y no desde la de invitados (No agrega valor anexar más screenshots ya que se trata del mismo servidor, el 10.50.0.2).

Desde cualquier red tiene que poder accederse a DMZ y a Internet, probemos:

Figura 9.4: Acceso a DMZ

Vemos que desde la LAN de servidores (10.50.0.0/16) podemos acceder correctamente a curly.tdiii.com, que es el equipo 10.200.0.1 de la DMZ, también lo hicimos desde todas las otras redes y también funciona correctamente (por supuesto curly.tdiii.com desde internet no resuelve la 10.200.0.1 sino la 5.5.5.5 quien después le aplica un destination NAT):

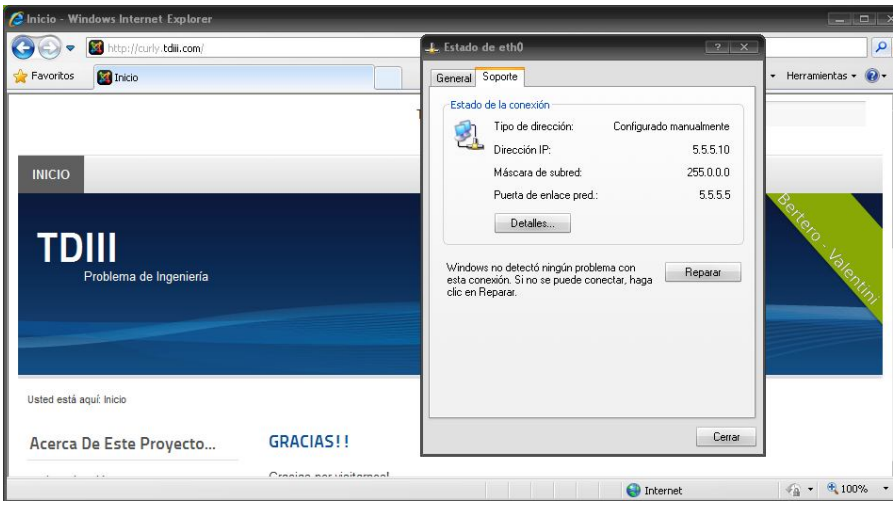

Figura 9.5: Acceso a DMZ

También corroboramos que desde todas las redes internas se puede acceder a internet y que desde la DMZ no se puede acceder a los servicios de LAN:

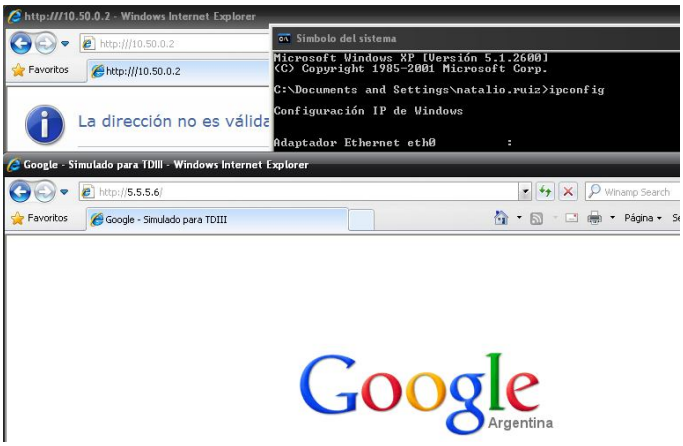

Figura 9.6: Acceso desde DMZ

9.2. Escaneo de puertos

Utilizamos la herramienta nmap para escaneo de puertos, nmap corre sobre sistemas GNU/Linux. Esta herramienta consulta los puertos abiertos de un host o red y de esta manera nos avisa que puertas de entrada hay a una

red, algunas son necesarias, otras son simplemente puntos débiles en la red, veamos como funciona la herramienta:

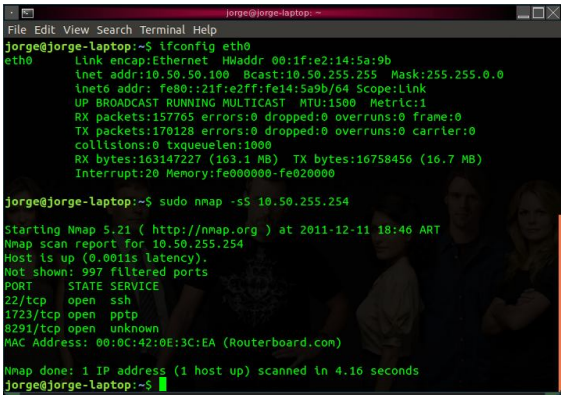

Figura 9.7: Escaneo de Puertos

Analicemos la información de la figura anterior, la IP de mi equipo (se ve en el comando "ifconfig") está en la red de servidores, pero particularmente en el segmento 10.50.50.0/24, que es la única porción de red desde la que se permite administrar los routers. Los puertos que se ven abiertos son: el 22, el 1723 y el 8291[2]. El puerto 1723 el router lo necesita para poder dar el servicio de PPTP, por eso no está filtrado, los otros dos sirven para administrar el router, tanto por SSH como por Winbox, pero, como bien se mencionó anteriormente en este párrafo, estamos en una red que admite la administración, intentemos por ejemplo desde la red de invitados...

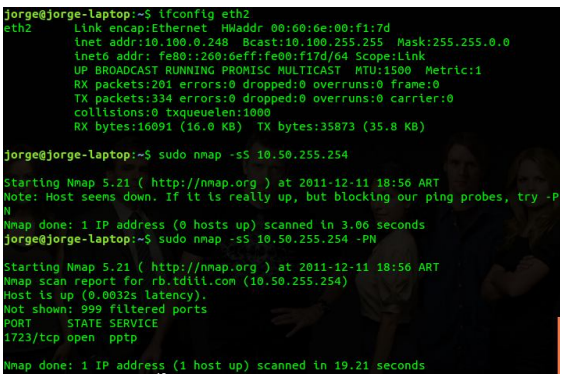

Figura 9.8: Escaneo de Puertos

[2]Los parámetros "sS" que se le pasan a nmap, no son arbitrarios o caprichosos, es para que analice TCP y UDP de manera lo suficientemente agresiva, tanto es así que requiere altos privilegios desde el cliente para ejecutarlo, es por eso que se invoca el comando "sudo" cuya acción es correr el siguiente comando con los mas altos privilegios del sistema.

Como se ve, ocurren dos cosas, en una primera instancia nmap nos dice que el host parece estar caído, esto es porque no se permite ping (ICMP) desde la red de invitados, entonces sale una advertencia que nos dice: "Parece que el host está caído, si no lo está y solo está bloqueando nuestras pruebas de ping, entonces ejecute nmap con el parámetro -PN". Hacemos caso a la instrucción y obtenemos el resultado, sólo se permite conectarse a una VPN a través de PPTP, de esta manera escaneamos todos los puertos corroborando que todo sea como se planificó.

Una herramienta muy útil es zenmap que es un frontend de nmap, pero que ya tiene preseteados algunos comandos ya parametrizados y listos para lanzar:

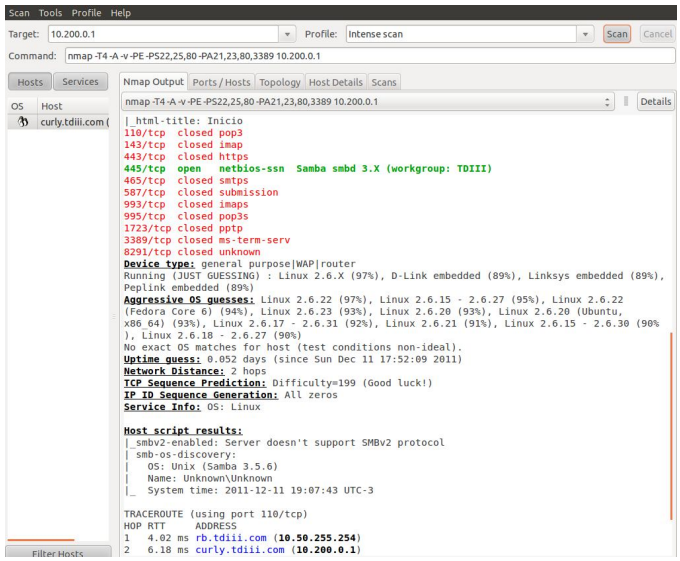

Figura 9.9: Escaneo de Puertos

9.3. Herramientas más completas

Como un trabajo mas fino de seguridad (en el que no nos involucraremos en este trabajo) se pueden utilizar otras herramientas que hacen escaneos muchísimo mas profundos y de otras cosas como protección antivirus, software espía y actualizaciones de seguridad de software, ejemplos de estas (Con licencia por IP escaneada) son Nessus y GFI Lan Guard.

Además hay montones de herramientas de seguridad, para diferentes cuestiones, escaneo de seguridad de contraseñas, de redes, juntar información y demás, pueden encontrarse muchas de ellas, algunas gratuitas y

otras pagas, en internet[3].

9.4. Fuerza Bruta

El método de ataque conocido como "Fuerza Bruta" sirve para obtener nombres de usuario y contraseñas, es un método algo arcaico (pero muy efectivo en redes que no se protegen contra él), y es un método de prueba y error automatizado, es decir, se utiliza un software al que se le pasan usuarios comunes (como admin, administrator, root, etc) o bien usuarios conocidos que se hayan podido obtener de una u otra manera y un "diccionario" de contraseñas, de esta manera, el software intenta validarse con todas las combinaciones posibles hasta que obtiene una conexión exitosa.

Escribiendo el documento se pensó mucho si debíamos resolver esto aquí o en el capítulo anterior en la configuración de firewall, pero creemos que mitigar este tipo de cuestiones ya no es de firewall sino de pruebas de seguridad de post producción, es por eso que mostramos como se realiza el filtrado en esta sección.

En esta red poseemos un servicio de validación que es crítico: el PPTP. Si un usuario malintencionado accede por fuerza bruta a PPTP está dentro de la LAN (Por más que podría filtrarse particularmente la VPN), para evitar los ataques por fuerza bruta, el método recomendado por mikrotik es, agregar al firewall las reglas (pseudocódigo):

1. Cuando se abre una conexión nueva a PPTP, se pasa la IP de origen a una Address List llamada **PPTP-Con1** por 1 minuto
2. Cuando se abre una conexión nueva a PPTP desde una IP de la Address List **PPTP-Con1**, se pasa la IP de origen a una Address List llamada **PPTP- Con2** por 1 minuto
3. Cuando se abre una conexión nueva a PPTP desde una IP de la Address List **PPTP-Con2**, se pasa la IP de origen a una Address List llamada **PPTP- Con3** por 1 minuto
4. Cuando se abre una conexión nueva a PPTP desde una IP de la Address List **PPTP-Con3**, se pasa la IP de origen a una Address List llamada **PPTP- Con4** por 1 minuto

[3] Siempre que se hagan pruebas que sea en redes controladas ya que muchas veces se pueden ocasionar daños, además muchas veces puede ser considerado una violvación de las legislaciones vigentes

5. Cuando se abre una conexión nueva a PPTP desde una IP de la Address List **PPTP-Con4**, se pasa la IP de origen a una Address List llamada **PPTP- Con5** por 1 minuto
6. Cuando se abre una conexión nueva a PPTP desde una IP de la Address List **PPTP-Con5**, se pasa la IP de origen a una Address List llamada **PPTP- BlackList** por 3 horas
7. Se rechaza TODA conexión a PPTP desde la Adress List **PPTP-BlackList**

Lógicamente los nombres de las Address Lists son arbirtrarios, también los tiempos y la cantidad de conexiones permitidas, pero con esas reglas, si alguien intenta desde internet 5 veces conectarse a PPTP a intervalos de menos de 1 minuto quedará bloqueado por 3 horas, esto significa, no podrá conectarse desde esa IP por 3 horas (y cambiar la IP de internet no siempre es un trámite sencillo), por lo tanto el atacante no puede hacer fuerza bruta en ese servicio[4]

9.5. Port Knocking

La técnica de seguridad conocida como "Port Knocking" consiste en utilizar, nuevamente, reglas de firewall combinadas con Address Lists para lograr una mayor seguridad.

Veámoslo con un ejemplo práctico, supongamos que se da un servicio (suficientemente crítico) a internet, digamos la administración del firewall por medio de winbox, de cierta manera, utilizamos el firewall para obligar a "tocar" una cierta combinación de puertos (generalmente 3) para llegar, esto se hace de la siguiente manera:

1. Cuando llega un paquete TCP al puerto 3456, se agrega la IP a la Address List **Golpeo-Primer-Puerta** por 1 minuto
2. Cuando llega un paquete TCP al puerto 4321, que viene de la Address List **Golpeo-Primer-Puerta**, se agrega la IP a la Address List **Golpeo-Segunda- Puerta** por 1 minuto
3. Aceptar todo tráfico a TCP 8291 que venga desde un equipo en la Address List **Golpeo-Segunda-Puerta** por 1 minuto

[4]Un diccionario bien poblado de contraseñas, posee alrededor de 20 millones (no es exageración, investigando descargamos un diccionario que poseía 17.965.793 claves, en solo 100 MB), lo que da a pensar, ya que, teniendo un bloqueo de 3 horas cada 5 intentos se podrían probar menos de 15000 en 1 año de trabajo constante. Ya es solo como curiosidad mencionar, que llevaría mas de 1300 años probarlas todas... Conclusión: ¡El método es bueno!

Así, el administrador del router debe primero intentar conectarse en el puerto 3456 (por supuesto sin éxito aparente), luego al 4321, recién entonces, su IP está habilitada para acceder al equipo por Winbox, una vez pasado un minuto, deberá volver a comenzar (por supuesto cuando ya haya establecido la conexión caera en una regla que acepte conexiones establecidas).

9.6. Buenas Prácticas

Se puede haber notado que los nombres de los servidores no son del todo "serios", sin embargo, es parte de las buenas prácticas de seguridad informática que un servidor no haga referencia a su función en la red, por ejemplo, si el servidor de RADIUS se llama freeradius, se sabe fácilmente que su función en la red es esa, y será el primer equipo a atacar para robar una base de usuarios, es por eso que en muchas empresas los servidores se llaman como dioses (hércules, dalila, neptuno, etc.), como modelos de autos (diablo, focus, aveo, etc.) o personajes de TV (Homero, Marge, Lisa, etc.), es por esta razón que elegimos esos nombres para los servidores:

larry: Servidor de archivos y web intranet - 10.50.0.2

schemp: Servidor de RADIUS - 10.50.0.1

curly: Servidor web público en DMZ - 10.200.0.1

moe: Servidor web simulando a Google - 5.5.5.6

Otra consideración, casi fundamental, es que un usuario de cualquier recurso informático, DEBE utilizar passwords fuertes, esto significa passwords que no sean obtenidas de un diccionario, que tengan 8 o más caractéres, que tengan mayúsculas, minúsculas, números y símbolos especiales (por ejemplo: M!P4ssw0rd$), de esta manera uno es menos vulnereable a sufrir un ataque por fuerza bruta (o simplemente por prueba y error manual).

Hay un tema más que vale mencionar, y roza las cuestiones legales más que las de seguridad informática, es lo que se llama "título", el título es un anuncio que se hace cuando uno se conecta a un dispositivo incluso antes de validarse, el título puede ser por ejemplo:

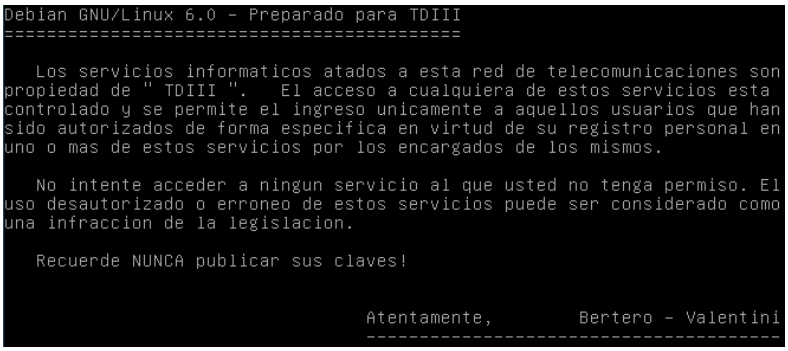

Figura 9.10: Título

Sin este anuncio, no se puede penalizar a un intruso, ya que la red no avisa que no se puede acceder.

Bibliografía

ALEGSA.COM.AR (Radius). Disponible en http://www.alegsa.com.ar/Dic/radius.php.

CISCO. CCNA 1 and 2. CISCO, 2008.

DARKNET.ORG.UK (Wireless Security Acronyms). Disponible en http://www.darknet.org.uk/2008/12/confused-by-wep-wpa-tkip-aes-other-wireless-security-acronyms/

FREERADIUS.COM (FreeRadius). Disponible en http://freeradius.org/doc/

FREERADIUS.ORG (Radius). Disponible en http://wiki.freeradius.org/RADIUS.

KIOSKEA.NET (DMZ). Disponible en http://es.kioskea.net/contents/protect/dmz-cloisonnement.php3.

LINUXHOMENETWORKING.COM (Linux Firewalls Using IPtables). Disponible en http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch14_:_Linux_Firewalls_Using_iptables.

MICROSOFT.COM (Network Security Methods). Disponible en http://windows.microsoft.com/es-ES/windows-vista/What-are-the-different-wireless-network-security-methods.

MOSQUERA, J. (Subredes). Disponible en http://www.monografias.com/trabajos76/computacion-informatica-subneteo/computacion-informatica-subneteo2.shtml.

SLICEOFLINUX (Virtualización). Disponible en http://sliceoflinux.com/virtualizacion.

SLIDEBOOM (Red Informática). Disponible en http://www.slideboom.com/presentations/137023/Qué-es-un-red-informática.

WIKIPEDIA (CSMA/CD). Disponible en http://es.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_detection.

WIKIPEDIA (Dirección IP). Disponible en http://es.wikipedia.org/wiki/Dirección_IP.

WIKIPEDIA (Firewall). Disponible en http://es.wikipedia.org/wiki/Cortafuegos_(informática).

WIKIPEDIA (Modelo OSI). Disponible en http://es.wikipedia.org/wiki/Modelo_OSI.

WIKIPEDIA (Máscara de red). Disponible en http://es.wikipedia.org/wiki/Máscara_de_red.

WIKIPEDIA (Router). Disponible en http://es.wikipedia.org/wiki/Router.

WIKIPEDIA (Virtualización). Disponible en http://es.wikipedia.org/wiki/Virtualización.

WIKIPEDIA (DMZ). Disponible en http://es.wikipedia.org/wiki/Zona_desmilitarizada_(informática).

Lista de acrónimos

AP ..... Access Point, Es el dispositivo que se utiliza para concentrar redes inalámbricas. Muchas veces se lo llama Punto de acceso en países hispanoparlantes

ASCII ..... American Standard Code for Information Interchange, Es un sistema de codificación de caracteres basado en el orden del alfabeto ingés

CSMACD .... Carrier Sense Multiple Access with Collision Detection, En castellano, .Acceso Múltiple por Sensado de Portadora con Detección de Colisiones", es una técnica usada en redes Ethernet para mejorar sus prestaciones.

DMZ ..... Demilitarized Zone, Es una zona de seguridad media de una red, tiene por característica principal no tener permitido abrir conexiones hacia la red de seguridad superior con la que convive

DSSS ..... Espectro de Dispersión de Secuencia Directa, Uno de los primeros estándares sobre redes inalámbricas

FCC ..... Federal Communications Commission, Ente encargado de gestionar las normas sobre comunicaciones

IANA ..... Internet Assigned Numbers Authority, Ente que controla el número para protocolos, el código de país de dominios de nivel primario y mantiene las asignaciones de direcciones IP.

ICANN..... Internet Corporation for Assigned Names and Numbers, Ente sin fines de lucro que vela por la seguridad, estabilidad e interoperabilidad de internet

RADIUS..... Remote Authentication Dial-In User Service, Es un servicio de validación y estadísticas de usuarios

ROI ..... Return Of Invest, El Retorno de la inversión (ROI por sus siglas en inglés)es una relación que compara el beneficio o la utilidad obtenida en relación a la inversión realizada.

TCO ..... Total Cost of Ownership, El coste total de propiedad (proveniente del término anglosajón Total Cost of Ownership), es un método de cálculo diseñado para ayudar a los usuarios y a los gestores empresariales a determinar los costes directos e indirectos, asi como los beneficios, relacionados con la compra de equipos o programas informáticos.

WLAN ..... Wireless Local Area Network, Término que se utiliza usualmente para referirse a redes Wi-Fi